UNIVERSIDAD COMPLUTENSE DE MADRID
FACULTAD DE DERECHO

TESIS DOCTORAL

Institucionalización de la protección de datos personales en Chile, referencias del caso español

MEMORIA PARA OPTAR AL GRADO DE DOCTOR

PRESENTADA POR

Emilio Alejandro Oñate Vera

Director

Manuel Sánchez de Diego Fernández de la Riva

Madrid

© Emilio Alejandro Oñate Vera, 2023

UNIVERSIDAD COMPLUTENSE DE MADRID
FACULTAD DE DERECHO

TESIS DOCTORAL

INSTITUCIONALIZACIÓN DE LA PROTECCIÓN DE DATOS PERSONALES EN CHILE, REFERENCIAS DEL CASO ESPAÑOL

Emilio Alejandro Oñate Vera

Tesis para optar al grado académico de Doctor en Derecho,
dirigida por el profesor Manuel Sánchez de Diego Fernández de la Riva

Madrid, 2022

UNIVERSIDAD COMPLUTENSE DE MADRID
FACULTAD DE DERECHO

TESIS DOCTORAL

INSTITUCIONALIZACIÓN DE LA PROTECCIÓN DE DATOS PERSONALES EN CHILE, REFERENCIAS DEL CASO ESPAÑOL

Emilio Alejandro Oñate Vera

Tesis para optar al grado académico de Doctor en Derecho,
dirigida por el profesor Manuel Sánchez de Diego Fernández de la Riva

Madrid

Para Alejandra y Josefina.

ÍNDICE

RESUMEN **15**
ABSTRACT **18**
OBJETO, METODOLOGÍA Y ESTRUCTURA **21**
Objetivo General **22**
Objetivos Específicos **22**
Metodología **24**
Preguntas de la Investigación **25**
Capítulo Primero **26**
Capítulo Segundo **27**
Capítulo Tercero **28**
Capítulo Cuarto **29**
Capítulo Quinto **30**
OBJECT, METHODOLOGY AND STRUCTURE **33**
General Objective **34**
Specific Objectives **34**
Methodology **36**
Research Questions **37**
Chapter One **37**
Second Chapter **39**
Third Chapter **40**
Chapter Four **41**
Chapter Five **42**
CAPÍTULO I -LA PROTECCIÓN DE DATOS COMO DERECHO FUNDAMENTAL **44**
La Dignidad Humana como sustento de los Derechos Fundamentales **44**
El Derecho a la Intimidad 48
El Derecho a la Privacidad y a la Vida Privada 53
Jurisprudencia del Tribunal Europeo de Derechos Humanos (TEDH) sobre la vida privada 55
Jurisprudencia de la Corte Interamericana de Derechos Humanos (CIDH) sobre la vida privada 58
Relación entre la Intimidad, la Vida Privada y el Derecho a la Protección de Datos 60
Aproximación al Derecho a la Protección de Datos a nivel internacional **67**
Antecedentes al Derecho a la Protección de Datos 67

Directrices de la OCDE de 1980 68
1. Principio de limitación de recogida 68
2. Principio de calidad de los datos 68
3. Principio de especificación de los fines 69
4. Principio de limitación de uso 69
5. Principio de salvaguarda de la seguridad 69
6. Principio de transparencia 69
7. Principio de participación individual 69
8. Principio de responsabilidad 69
El Derecho a la protección de datos en Europa y Latinoamérica 70
El Derecho a la Protección de Datos en Colombia 74
El Derecho a la Protección de Datos en Perú 75
El Derecho a la Protección de Datos en México 75
El Derecho a la Protección de Datos en Chile 76
Derecho de acceso 80
Derecho a la modificación o rectificación 81
Derecho de cancelación o eliminación 82
Derecho de bloqueo 82
Otros derechos 83
El Reconocimiento constitucional del Derecho a la Protección de Datos en Chile 84
La Protección de Datos en la OCDE 87
La Actualización del Convenio 108 88
La Protección de Datos en el Tratado de la UE y en el Tratado de Funcionamiento de la Unión Europea 91
El Reglamento General de Protección de Datos Personales RGPD 98
Objeto del RGPD 98
Propósitos del RGPD 99
Ámbito de aplicación del RGPD 99
Nuevos términos definidos por el RGPD 100
La Autoridad de Control en el RGPD 100
El Consentimiento del titular de los datos en el RGPD 101
Contenido y Alcance del tratamiento en el RGPD 101
El Tratamiento de datos de niñas y niños en el RGPD 102
El Derecho de Rectificación en el RGPD 102
El Derecho al Olvido 103
El caso Costeja v. Google 103
El Derecho al Olvido en el RGPD 106

El Derecho de Portabilidad 109
El Derecho de Oposición 110
La Protección de Datos Personales en España 113
Anclaje constitucional 113
Desarrollo legislativo en España: Tres Leyes Orgánicas de protección de datos personales 115
No es un derecho absoluto. La necesaria proporcionalidad 116
Innovaciones en la normativa española de protección de datos personales. 117
Derecho a ser informado con transparencia 117
Derecho de acceso 118
Designación de un Delegado de Protección de Datos 119
Tratamiento de datos de contacto de empresarios y profesionales 120
Derechos digitales 120
Derecho a la neutralidad en Internet 121
Derecho de acceso universal 121
Derecho a la seguridad digital 122
Derecho a la desconexión digital en el ámbito laboral 122
Derechos a la intimidad frente al uso de dispositivos de videovigilancia y de grabación de sonidos en el lugar de trabajo 123
Derecho a la intimidad ante la utilización de sistemas de geolocalización en el ámbito laboral 123
Derecho al olvido 124
Derecho al testamento digital. 125
Consideraciones finales del Capítulo 126
CAPÍTULO II- LA TUTELA DE LA PROTECCIÓN DE DATOS Y SU JURISPRUDENCIA ANTE EL TRIBUNAL DE JUSTICIA DE LA UNIÓN EUROPEA 127
Protección de los Derechos Fundamentales. Garantías en sentido amplio. 127
Garantías normativas 127
Procedimientos jurídicos específicos 128
Institucionales – Autoridad de Control 129
La reclamación ante la autoridad de control y la tutela judicial efectiva en el contexto europeo 130
El derecho de reclamación ante una Autoridad de Control 130
El derecho a presentar reclamaciones ante la autoridad de control 133
Reclamación, Transparencia e Información 135
El Derecho a la tutela judicial efectiva 137
La jurisprudencia del Tribunal de Justicia de la Unión Europea (TJUE) sobre protección de datos 139

Sentencia T-452/17 – TL/SEPD, del 28 de junio de 2018 140
Sentencia C-207/16 – Ministerio Fiscal, de 2 de octubre de 2018 141
Sentencia C-210/16, Wirstschaftsakademie Schleswig-Holstein, de 5 de junio de 2018 145
Sentencia C-25/17 Jehovan Todistajat, de 10 de julio de 2018 154
Sentencia C-40/17- Fashion ID, de 29 de julio de 2019 160
Sentencia C-136/17- GC y otros, de 24 de septiembre de 2019 167
Sentencia C-345/17 - Buivids, de 14 de febrero de 2019 178
Sentencia C-507/17 - Google (Portée territoriale du déréférencement), de 24 de septiembre de 2019 . 184
Sentencia C-673/17 - Planet49, de 1 de octubre de 2019 195
Sentencia C-708/18 - Asociaţia de Proprietari bloc M5A-ScaraA, de 11 de diciembre de 2019 202

Consideraciones finales 207

CAPÍTULO III LA PROTECCIÓN DE DATOS EN AMERICA LATINA 210

Introducción 210

Estándares para la Protección de Datos en los países Iberoamericanos de la Red Iberoamericana 212

Principios de la Protección de Datos de la Organización de Estados Americanos (OEA) 217

Principio Uno: Finalidades Legítimas y Lealtad 218
Principio Dos: Transparencia y Consentimiento 220
Principio Tres: Pertinencia y Necesidad 220
Principio Cuatro: Tratamiento y Conservación Limitados. 221
Principio Cinco: Confidencialidad. 222
Principio Seis: Seguridad de los Datos. 222
Principio Siete: Exactitud de los Datos. 223
Principio Ocho: Acceso, Rectificación, Cancelación, Oposición y Portabilidad. 223
Principio Nueve: Datos Personales Sensibles. 224
Principio Diez: Responsabilidad. 225
Principio Once: Flujo Transfronterizo de Datos y Responsabilidad. 226
Principio Doce: Excepciones. 227
Principio Trece: Autoridades de Protección de Datos. 228

La Protección de datos en Estados Unidos 229

Ley de Privacidad del Consumidor de California 232

La Protección de Datos en las Constituciones Latinoamericanas 233

Argentina 233
Bolivia 234
Brasil 235
Chile 235

Colombia....235
Costa Rica....236
Cuba....237
Ecuador....238
El Salvador....238
Guatemala....239
Honduras....239
México....240
Nicaragua....240
Panamá....241
Paraguay....242
Perú....242
República Dominicana....242
Uruguay....243
Venezuela....243

Algunas consideraciones sobre el tratamiento constitucional de la Protección de Datos en Latinoamérica....244

La protección de Datos en las Legislaciones Latinoamericanas....245

Argentina....245
Brasil....248
Chile....254
Colombia....260
Costa Rica....263
Ecuador....265
El Salvador....268
Guatemala....270
Honduras....271
México....272
Nicaragua....286
Panamá....289
Perú....292
República Dominicana....296
Uruguay....300

Cuadro comparado de legislación en protección de datos y autoridades de control en Latinoamérica....305

Consideraciones Finales....308

CAPÍTULO IV LA AUTORIDAD DE CONTROL PARA LA PROTECCIÓN DE DATOS Y SU INDEPENDENCIA....311

La Independencia en las Autoridades de Control....312

Elementos de las entidades independientes 316
Estabilidad versus Legitimidad y Tecnicismo versus Armonía, como elementos de la Independencia 317
Principios OCDE para mejores prácticas de las agencias independientes 321
1. Claridad en los roles 321
2. Evitar la influencia indebida y mantener la confianza 322
3. Toma de decisiones y estructura de órganos de gobierno para reguladores independientes 324
4. Rendición de cuentas y transparencia 325
5. Participación y compromiso de los actores interesados 327
6. Financiamiento 328
7. Evaluación del desempeño 329
La Autoridad de Control en la Directiva 95/46 del Consejo de Europa 330
La Autoridad de Control en el Reglamento General de Protección de Datos RGPD 679/2016 334
Elementos de la independencia de los miembros y de la propia Autoridad de Control en el RGPD 337
Elementos que estructuran la independencia de los miembros o integrantes de la Autoridad de Control 338
Elementos que estructuran la independencia en el funcionamiento de la Autoridad de Control 340
Competencia, Funciones y Poderes de la Autoridad de Control 342
Competencia 342
Funciones 348
a) Las Funciones coercitivas 350
b) Las Funciones de prestación y promoción 353
c) La Función de Cooperación 357
Poderes 358
A. Los Poderes de Investigación 359
B. Los Poderes Correctivos 360
C. Poderes de Autorización y Consultivos 360
El Tratamiento Internacional y Transfronterizo de datos Personales y la Autoridad de Control 361
Transferencias Basadas en un Nivel de Protección Adecuado (artículo 45 del RGPD) 363
Transferencias mediante garantías adecuadas (artículo 46 del RGPD) 365
Transferencias con Excepciones para situaciones específicas 367
Tratamiento Transfronterizo de Datos 368
Análisis comparado de la tipología de las Agencias de Protección de Datos 370
1. Modelo único o mixto 371
Países de la Unión Europea 371
Países de la Organización para la Cooperación y el Desarrollo Económicos - OCDE 376
Países miembros de la Red Iberoamericana de Protección de Datos 380

2. Estructura Colegiada o Autoridad Unipersonal – Autónoma o Dependiente 384
Consideraciones sobre la Autoridad de Control en la Experiencia Comparada 388
La Autoridad de Control en España 389
Consideraciones Finales..... 398
CAPÍTULO V HACIA LA INSTITUCIONALIZACIÓN DE LA PROTECCIÓN DE DATOS PARA CHILE..... 402
La Privacidad y la protección a la Vida Privada en las Constituciones chilenas..... 402
Reglamento Constitucional de 1812..... 402
Constitución de 1818..... 403
Constitución de 1822..... 403
Constitución de 1828..... 404
Constitución de 1833..... 404
Constitución de 1925..... 405
Constitución de 1980..... 406
Historia de la Ley sobre protección a la vida privada N° 19.628..... 409
Proyecto de ley sobre Protección a la Vida Privada 410
Etapas de la Tramitación Legislativa..... 413
Reformas a la Ley 19.628..... 423
a) Ley N°19.812 423
b) Ley N°20.463 424
c) Ley N°20.521 424
d) Ley N°20.575 425
Hacia una nueva Ley de Protección de Datos en Chile (Boletines números 11.144-07 y 11.092-07 refundidos)..... 434
Hacia una Autoridad de Control para la Protección de Datos para Chile 450
La Agencia de Protección de Datos..... 451
La votación en la Comisión sobre la Autoridad de Control 460
Hacia una Autoridad de Control Independiente para la Protección de Datos Personales 466
Las Agencias Reguladoras Independientes en Chile..... 467
a) Las Superintendencias y otras entidades similares 467
Órganos con autonomía constitucional..... 471
b) Entidades Colegiadas 472
El nuevo artículo 15 Bis de Ley N° 19.496 sobre Protección de los Derechos del Consumidor: la competencia del SERNAC 481
Diseño Organizacional y Régimen de Responsabilidad de una Autoridad de Protección de Datos para Chile..... 484

Régimen de Responsabilidad 485
Una Institucionalidad para la Protección de Datos en el Marco de una nueva Constitución 486
Evolución política chilena hacia una nueva Constitución 486
Afrontando un nuevo derecho fundamental a la protección de datos personales 488
El Habeas data en Chile y Latinoamérica 489
Consideraciones finales 491
Argumentos a favor de un modelo único 493
Argumentos a favor de un órgano colegiado 495
En relación a si la autoridad de control debe configurarse como un órgano colegiado o pluripersonal, es posible sistematizar los siguientes argumentos: 495
Argumentos a favor de un órgano unipersonal 495
Propuesta 496
CONCLUSIONES 497
Primera Parte 497
Segunda Parte 502
BIBLIOGRAFÍA 508
REFERENCIAS PROPIAS 517
JURISPRUDENCIA 517

RESUMEN

El presente trabajo de investigación estudia y propone estándares para establecer una Autoridad de Control en materia de protección de datos para Chile, tomando como referencia la experiencia comparada, principalmente europea y especialmente española. Se analiza el desarrollo de la protección de datos personales como derecho fundamental, sustancialmente en la Europa continental, abordando la relación de este derecho con otros derechos fundamentales, como el derecho a la intimidad y el respeto y protección a la vida privada.

Producto del vertiginoso desarrollo de las tecnologías de la información, la inteligencia artificial, el masivo almacenamiento de datos y su tratamiento en los sectores públicos y privados, así como su transferencia a otros países, existe una situación en la que las personas pueden quedar a merced de quienes manejan la información que les concierne. Para protegerlas se ha configurado, primordialmente en Europa, un derecho fundamental que tiene una independencia y autonomía propias, lo que nos lleva a analizar la normativa europea. Entre las normas europeas más importantes encontramos el Convenio 108 del Consejo de Europa (28/01/1981); la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre y; el Reglamento General de Protección de Datos 2016/679 de 27 de abril. Este marco jurídico europeo se completará con las futuras normas de la la Unión Europea: el Reglamento Europeo de Servicios Digitales y el Reglamento de Mercados Digitales. Revisaremos y analizaremos el objeto, propósitos, ámbito de aplicación de la protección de datos personales, estudiando los denominados derechos ARCO (Acceso, Rectificación, Cancelación y Oposición), completados en el Reglamento 2016/679 con otros derecho como derecho al olvido digital y el derecho a la portabilidad. Este estudio se completa con la revisión y estudio de la jurisprudencia sobre protección de datos desarrollada desde el 2018 en adelante por el Tribunal de Justicia de la Unión Europea, donde se define el sentido y alcance, así como las formas de aplicación de conceptos como el "responsable del tratamiento" que debe ser interpretado en sentido amplio, que incluye tanto al administrador de una página web o de una red social como a los proveedores de ésta, o a los denominados motores de búsqueda, y que del mismo modo, refuerza las facultades de la Autoridad de Control en protección de datos para regular las sucursales de las empresas que realicen tratamiento de datos personales o actividades afines, aun cuando la matriz de dicha empresa se encuentre ubicada fuera de un Estado miembro de la Unión, entre otras materias.

El trabajo que aquí se resume aborda también una revisión de la regulación normativa en el ámbito latinoamericano de la protección de datos a nivel constitucional y legal. De este análisis es posible colegir que la regulación de la protección de datos personales en las constituciones latinoamericanas es diversa, y en muchos casos más bien deriva de una interpretación o extensión de los derechos a la intimidad, vida privada, honra o imagen que de una mención explícita que lo reconozca. En otros casos, más que una referencia o regulación a la protección de datos, las Cartas Políticas se refieren al habeas data, como un mecanismo o acción para tutelar el derecho a la protección de datos, aun cuando este no tenga un tratamiento expreso. De las legislaciones de protección de datos revisadas, cualquiera sea el orden o estructura en que se configuren, Títulos, Capítulos o Secciones, en general se distinguen como elementos centrales: una conceptualización de términos en donde destacan las definiciones de datos personales y datos sensibles; los principios en que debe sustentarse el tratamiento de datos; los derechos de los titulares de los datos; la transferencia de datos; la autoridad de control en la

materia; y la acción o procedimiento de tutela, así como las sanciones a que se verán expuestas las entidades públicas y privadas que no cumplan con sus disposiciones.Si bien los países 5latinoamericanos han realizado esfuerzos para generar directrices comunes en materia de protección de datos, como los Estándares de la Red Iberoamericana de Protección de Datos o la actualización de los Principios para el tratamiento de datos de carácter personal de la Organización de Estados Americanos OEA, del 9 de abril del año 2021, estas constituyen normas de *soft law* que no son vinculantes para los Estados miembros.

La presente investigación se centra también en el estudio de las Autoridades de Control en materia de protección de datos, analizando primero la anterior regulación europea contenida en la Directiva 95/46 del Consejo de Europa y el actual Reglamento General de Protección de Datos de la Unión Europea 2016/679, que de manera mucho más completa y especifica regula los objetivos, propósitos, ámbito de aplicación, así como las competencias, poderes y funciones de tales autoridades entre los Estados de la Unión. Así mismo, se hace una revisión de los criterios comparados para su establecimiento, poniendo especial énfasis en lo que se denomina un modelo único o mixto, es decir, si tales organismos de control regulan únicamente la protección de datos y su adecuado tratamiento, o si además de ello son entidades encargadas de la regulación, promoción y tutela del derecho de acceso a la información pública respectivamente. Concluyendo, según el análisis comparado, que en los países de la Unión Europea, e incluyendo a los países integrantes de la Organización para la Cooperación y Desarrollo Económico y a los que integran la Red Iberoamericana de Protección de Datos, una amplia mayoría de entidades de control en el mundo se configuran bajo el denominado modelo único.

También se analiza comparativamente, a nivel de la señalada instancia iberoamericana, la forma en que se estructuran orgánicamente las autoridades de control desde la perspectiva de sus gobiernos corporativos, esto es, si son autoridades unipersonales o colegiadas, constatando que, en esta instancia, integrada por más de una decena de países, solo tres configuran sus agencias de control como organismos pluripersonales, que son los casos de Brasil, México y Uruguay. Otro de los criterios que se desarrollan en el presente trabajo apunta al carácter independiente de las autoridades de control para la protección de datos. Esta independencia que se encuentra expresamente señalada en la normativa europea no es tan nítida a nivel latinoamericano, en efecto, países como Costa Rica y Perú tienen entidades de control dependientes de la autoridad política, concretamente del Ministerio de Justicia y Paz de Costa Rica y del Ministerio de Justicia Peruano.

También se revisa la más reciente legislación española en la materia, contenida en Ley Orgánica 3/2018 de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, centrando el análisis en la regulación de la Agencia Española de Protección de Datos. Luego, se realiza un análisis de las autoridades independientes, como se les denomina en el sistema español, y que en el derecho comparado admiten diferentes denominaciones: en Reino Unido se les ha dado el nombre de *quangos o quasi autonomous non governmental organisations*, en Estados Unidos, *independent agencies*, en Francia se les denomina *autorités administratives indépendantes*, en Alemania, *funktionale Selbstverwaltungsträgern*. Cualquiera sea su denominación, estas entidades independientes han sido estructuradas sobre la base de disponer de un régimen mayor de independencia del poder central, y que en el sistema de la Administración Pública chilena se les denomina

organismos autónomos. Entre los elementos que configuran esta independencia se destacan la neutralidad política, la especialización técnica y la eficacia, que tienen como propósito que las decisiones sean adoptadas con prescindencia de las preferencias coyunturales de un Gobierno determinado, permitiendo sostener una política pública consistente en el largo y en el corto plazo, siendo una de las manifestaciones más evidentes de aquello, más que el reconocimiento constitucional de la autonomía, como puede ocurrir en Chile, la manera en que son generadas sus autoridades superiores, así como, especialmente, su régimen de remoción, incompatibilidades y dedicación. Igualmente se revisan los principios sobre mejores prácticas para la Gobernanza de los Reguladores o agencias independientes establecidos por la Organización para la Cooperación y Desarrollo Económico, que son lineamientos para fortalecer su diseño institucional y, por tanto, buscan mejorar su desempeño.

La última parte de esta investigación doctoral se refiere a la necesidad de avanzar hacia la institucionalización de la protección de datos en Chile, considerando la historia constitucional chilena, la que desde sus primeros Reglamentos Constitucionales (1812) expresó preocupación por la privacidad de las personas, hasta el reconocimiento, en el año 2018, de la protección de datos como derecho fundamental en el N° 4 del artículo 19 de la aún vigente Carta Política. Así mismo, se realiza un examen crítico de la ley sobre Protección a la Vida Privada N° 19.628, del año 1999, que regula la protección de datos personales, legislación que no solo ha perdido vigencia y eficacia, sino que además tiene importantes déficits en su contenido, especialmente por la ausencia de una autoridad de control que promueva y regule la protección de datos en Chile. De igual forma se estudia el proyecto de ley que desde el año 2017 se encuentra en primer trámite constitucional en el Senado chileno, que crea una nueva institucionalidad para la protección de datos y que ha sido zigzagueante en determinar quien será la autoridad de control en materia de protección de datos en Chile y cuáles serán los elementos para su configuración. En este sentido, se hace una revisión de veintidós agencias regulatoria existentes en el sistema chileno, categorizándolas en tres grupos: las superintendencias, los órganos constitucionalmente autónomos y las entidades regulatorias colegiadas, definiendo criterios de comparación que contribuyan a determinar cómo y bajo qué características debería constituirse una Autoridad de Control para la protección de datos en el sistema chileno.

Considerando la revisión realizada, se concluye que lo más aconsejable es que esta entidad aborde exclusivamente la protección de datos, y que teniendo en cuenta el *momentum* constitucional por el que atraviesa Chile, existe una oportunidad inigualable para que el nuevo texto constitucional disponga que a través de la respectiva ley se estructure una entidad o autoridad de control encargada no solo de proteger y fiscalizar tanto a instituciones públicas como privadas en el cumplimiento efectivo del respeto a la protección de datos personales como derecho fundamental, sino además se encargue de su promoción y del desarrollo de acciones preventivas para su adecuado resguardo.

Por ultimo es importante señalar en este resumen, que la presente investigación se realiza hasta el mes de septiembre del año 2021, aunque se han incorporado algunas referencias puntuales posteriores.

ABSTRACT

This research of this thesis studies and proposes standards to establish a Control Agency for data protection in Chile, taking as a reference the comparative experience of principally Europe and especially Spain. The analyses of data protection development as a fundamental right substantially in continental Europe, together with addressing the relationship of this right with other fundamental rights, such as the right to privacy, and the respect/protection of private life.

As a result of the vertiginous development of information technologies, artificial intelligence, the massive storage of data and its treatment in the public and private sectors, as well as its transfer to other countries, there is a situation in which people can be left at the mercy of those who handle the information that concerns them. To protect them, a fundamental right has been configured, primarily in Europe, that has its own independence and autonomy, which leads us to analyze European regulations. Among the most important European standards we find Convention 108 of the Council of Europe (01/28/1981); Directive 95/46/CE of the European Parliament and of the Council, of October 24 and; the General Data Protection Regulation 2016/679 of April 27. This European legal framework will be completed with the future regulations of the European Union: the European Regulation on Digital Services and the Regulation on Digital Markets. We will review and analyze the object, purposes, scope of application of the protection of personal data, studying the so-called ARCO rights (Access, Rectification, Cancellation and Opposition), completed in Regulation 2016/679 with other rights such as the right to digital oblivion and the right to portability. This study is completed with the review and study of the jurisprudence on data protection developed from 2018 onwards by the Court of Justice of the European Union, where the meaning and scope are defined, as well as the forms of application of concepts such as the "responsible for the treatment" that must be interpreted in a broad sense, which includes both the administrator of a web page or a social network and its providers, or the so-called search engines, and that in the same way, reinforces the powers of the Data Protection Control Authority to regulate the branches of companies that process personal data or related activities, even when the parent company of said company is located outside a Member State of the Union, among other matters.

The work summarized here also addresses a review of the normative regulation in the Latin American field of data protection at the constitutional and legal level. From this analysis it is possible to deduce that the regulation of the protection of personal data in Latin American constitutions is diverse, and in many cases derives rather from an interpretation or extension of the rights to privacy, private life, honor, or image than from an explicit mention that recognizes the same. In other cases, more than a reference or regulation to data protection, the Political Letters refer to habeas data, as a mechanism or action to protect the right to data protection, even when it does not have a direct mention. In general the following are distinguished as central elements in the revised data protection laws, regardless of the order or structure in which they are configured (Titles, Chapters or Sections): a conceptualization of terms where the definitions of personal data and sensitive data stand out; the principles on which data processing must be based; the rights of data owners; data transfer; the control

authority in the matter; and the habeas data actions, as well as the sanctions to which public and private entities that do not comply with its provisions will be exposed.

Although Latin American countries have made efforts to generate common guidelines on data protection, such as the Standards of the Ibero-American Data Protection Network or the updating of the principles for the processing of personal data of the OAS, from the past April 9, 2021, these constitute soft law regulations that are not binding on the Member States.

This research also focuses on the study of the Control Agencies in terms of data protection, first analyzing the past European regulation contained in Directive 95/46 of the Council of Europe and the current General Data Protection Regulation of the Union. European 2016/679, which in a much more complete and specific way regulates the objectives, purposes, scope of application, as well as the jurisdictions, powers and functions of such authorities among the States of the Union. Likewise, a review of the comparative criteria for its establishment is made, placing special emphasis on what is called a single or mixed model, that is, if such control bodies regulate only data protection and its adequate processing or if in addition of this, they are entities in charge of the regulation, promotion and protection of the right of access to public information, respectively. According to the comparative analysis that in addition to the countries of the European Union also includes the member countries of the Organization for Economic Cooperation and Development and those that make up the Ibero-American Data Protection Network, a conclusion is reached in the sense that a large majority of control entities in the world are configured under the so-called single model.

The way in which the Control Agencies are organically structured from the perspective of their corporate governments, that is, whether they are sole proprietorships or collegiate authorities, is also analyzed comparatively at the level of the aforementioned Ibero-American instance, noting that, in this instance, made up of more than a dozen countries, only three set up their control agencies as multi-person bodies, which are the cases of Brasil, Mexico and Uruguay. Other criteria that are developed in this work point to the independent nature of the Control Agencies for data protection, this independence that is expressly indicated in the European regulations is not so clear at the Latin American level, in effect, countries such as Costa Rica and Peru have control entities dependent on political authority, specifically the Costa Rican Ministry of Justice and Peace and the Peruvian Ministry of Justice.

The most recent Spanish legislation on the matter contained in Organic Law 3/2018 of December 5, on the Protection of Personal Data and guarantee of digital rights, is also reviewed, focusing the analysis on the regulation of the Spanish Agency for Data Protection. Then, an analysis is made of the independent authorities as they are called in the Spanish system and that in comparative law admit different denominations; in the United Kingdom they have been given the name of quangos or quasi autonomous non-governmental organizations, in the United States, independent agencies, in France they are called *autorités administrativees indépendantes*, in Germany, *funktionale Selbstverwaltungsträgern*. Whatever their name, these independent entities have been structured on the basis of having a greater regime of independence from the central power, and that in the Chilean Public Administration system they are called autonomous bodies. The following elements that make this independence stand out are indicated: political neutrality, technical specialization, and efficiency. There purpose is that decisions are adopted regardless of the situational preferences

of a given government, allowing the maintenance of a consistent public policy in the long and short term, being one of the more obvious manifestations of the latter, more than the constitutional recognition of autonomy, as can happen in Chile, the way in which its superior authorities are generated, as well as, especially, their regime of removal, incompatibilities, and dedication. Likewise, the principles on best practices for the Governance of Regulators or independent agencies established by the Organization for Economic Cooperation and Development are reviewed, which are guidelines to strengthen their institutional design and, therefore, seek to improve their performance.

The last part of this doctoral research refers to the need to move towards the institutionalization of data protection in Chile, considering the Chilean constitutional history, which from its first Constitutional Regulations (1812) expressed concern for the privacy of people until the recognition, in 2018, of data protection as a fundamental right in No. 4 of article 19 of the Political Charter still in force. Likewise, a critical examination is made of the Law on Protection of Private Life No. 19,628, of the year 1999, which regulates the protection of personal data, legislation that has not only lost validity and effectiveness, but also has significant deficits in its content, especially due to the absence of a control authority that promotes and regulates data protection in Chile. In the same way, the bill that since 2017 is in the first constitutional process in the Chilean Senate that creates a new institutionality for data protection and that has been zigzagging in determining who will be the control authority in matters of data, is studied, as well as data protection in Chile and what will be the elements for its configuration. In this sense, a review of twenty-two existing regulatory agencies in the Chilean system is made, categorizing them into three groups; the superintendencies, the constitutionally autonomous bodies and the collegiate regulatory entities, defining a comparison criterion that contributes to determining how and under what characteristics a Control Authority for data protection in the Chilean system should be constituted.

Considering the review carried out, the conclusion reached is that the most advisable option for this entity is to deal exclusively with data protection and that taking into account the constitutional momentum that Chile is going through, there is an unparalleled opportunity for the new constitutional text to provide this through the respective law, where an entity or control authority will be structured in charge not only of protecting and supervising both public and private institutions in the effective fulfillment of respect for the protection of personal data as a fundamental right, but also in charge of its promotion and the development of preventive actions for proper protection.

Finally, it is important to point out in this summary that this research is carried out until September 2021, although some subsequent specific references have been incorporated.

OBJETO, METODOLOGÍA Y ESTRUCTURA

En Chile se dicta en el año 1999 la Ley N° 19.628 sobre Protección a la Vida Privada[1], que a pesar de su denominación, regula específicamente la protección de datos de carácter personal. Esta legislación pionera en Latinoamérica en esta materia ha quedado desfasada y con escasa operatividad, no solo por la vertiginosidad de las transformaciones y cambios tecnológicos que se han producido desde su entrada en vigor hasta la fecha, tales como el *big data*, las redes sociales o la inteligencia artificial, sino también por la ausencia en dicha legislación de una entidad que regule y promueva la protección de datos personales como derecho fundamental.

A nivel constitucional, a diferencia de otros países de la región, en Chile recién en el año 2018 se reconoce como derecho fundamental la protección de datos personales, reconocimiento que, sin embargo, no ha impulsado la indispensable norma legislativa en la materia[2].

Desde el año 2017 se tramita en el Congreso Nacional chileno[3], un proyecto de ley que regula la protección y el tratamiento de datos personales, creando además una agencia o entidad a cargo de su regulación. Este proyecto de ley ha tenido una lenta tramitación en el Congreso, encontrándose aún en primer trámite constitucional, sin que en el actual contexto mundial de la pandemia se avizore un significativo avance, por lo que todo indica que esta trascendental discusión será postergada y abordada por un nuevo gobierno y congreso, en efceto, en el mes de noviembre del año 2021 se realizaron elecciones presidenciales y parlamentarias, cuyas nuevas autoridades asumirán en marzo próximo.

A lo anterior se suma el contexto político y social por el que atraviesa Chile, que ha desembocado en un proceso constituyente único en su historia, que implica la elaboración de un nuevo texto constitucional a través de una Convención Constitucional integrada por 155 convencionales constituyentes, que fueron electos el 15 y 16 de mayo del año 2021, paritaria (78 hombres y 77 mujeres), con integración de los pueblos originarios (17 escaños reservados para representantes de las distintas etnias indígenas)[4] y que tienen el plazo total de un año desde su instalación, el 4 de julio pasado , para redactar una nueva Carta, la que luego debe ser aprobada por la ciudadanía a través de un plebiscito ratificatorio[5].

Si bien estas circunstancias implican un retraso en la reconfiguración de una nueva institucionalidad para la protección de datos, a la vez representan una oportunidad para dotar de mayor vigencia y eficacia a la protección de datos personales, por cuanto en la nueva

1 Ver en: https://www.bcn.cl/leychile/navegar?idNorma=141599 consulta realizada el 24 de mayo de 2021.

2 Con fecha 16 de junio de 2018 se publicó en el Diario Oficial la ley 21.096, que consagra la protección de datos personales como garantía constitucional, en el numeral 4° del artículo 19 de la Constitución chilena. Ver en: Ley-21096 16-Jun-2018 Ministerio Secretaría General de la Presidencia - Ley Chile - Biblioteca del Congreso Nacional (Bcn.Cl) consulta realizada el 24 de mayo de 2021.

3 Ver en: https://www.camara.cl/ legislacion/ProyectosDeLey/ tramitacion.aspx?prmID=11661&prmBoletin=11144-07 consulta realizada el 24 de mayo de 2021.

4 Ver en: https://www.senado.cl/conozca-de-que-distritos-provendran-los-17-escanos-reservados-para/senado/2020-12-29/153330.html consulta realizada el 24 de mayo 2021.

5 Ver en: https://www.bcn.cl/procesoconstituyente/cronograma consulta realizada el 24 de mayo de 2021.

Constitución deberán reestructurarse los derechos ya establecidos, así como incorporarse nuevos derechos fundamentales, con sus respectivos instrumentos de tutela o garantía, siendo el caso de la protección de datos uno de ellos, con el establecimiento de su respectiva autoridad de control.

Por su parte, España cuenta desde hace ya varias décadas con una institucionalidad que se hace cargo de la protección de datos, a través de la Agencia Española de Protección de Datos[6], que se constituye como un referente en la materia y cuyo desarrollo y experiencias se transforman en un modelo a seguir no solo para Chile, también para toda Latinoamérica.

Objetivo General

La investigación doctoral que aquí se presenta tiene como objetivo general proponer las bases para el establecimiento de una Autoridad de Control en materia de protección de datos para Chile, tomando como referencia la experiencia comparada principalmente europea y en especial española, con la Agencia de Protección de Datos (AEPD) de ese país, así como la experiencia latinoamericana, especialmente con la entrada en vigor de las nuevas legislaciones en Brasil y Ecuador, lo que permitirá institucionalizar la protección de datos personales en Chile. En este trabajo se analizarán comparativamente las entidades encargadas de regular la protección de datos en diversos países y los criterios sobre los cuales debe configurarse una agencia reguladora.

Objetivos Específicos

Para el desarrollo del objetivo general, se proponen los siguientes objetivos específicos:

1. Analizar la protección de datos personales como derecho fundamental, desde sus orígenes en la Europa continental, pasando antes por *the right to privacy* (el derecho a ser dejado solo o en paz) que surge en Estados Unidos, hasta su regulación más reciente a través del Reglamento Europeo de Protección de Datos Personales (RGPD) 2016/679. Del mismo modo, se analizará su relación con la privacidad y la intimidad, entendiendo que son derechos similares pero diversos. En este sentido, se buscará determinar cuál es el contenido y alcance de la protección de datos, para verificar si implica o no un límite para que los datos o información de un individuo no puedan ser tratados sin su consentimiento, o si además incluye la facultad de su titular de disponer libremente de estos, controlando su disposición o incluso persiguiendo sus datos si es necesario.
   Se estudiará también si existe una relación o vínculo común entre la protección de datos y el derecho de acceso a la información pública.

[6] https://www.aepd.es/es. A nivel autonómico y dentro del ámbito de competencias de cada Comunidad Autónoma existen en la actualidad la Autoridad Catalana de Protección de Datos (2002), la Agencia Vasca de Protección de Datos (2004) y el Consejo de Transparencia y Protección de Datos de Andalucía (2014).

Así mismo se examinarán los denominados derechos ARCO (Acceso, Rectificación, Cancelación y Oposición), a los que habrá que agregar el derecho al olvido digital y el derecho a la portabilidad de los datos, incorporados en el RGPD.

2. Revisar y sistematizar la jurisprudencia del Tribunal de Justicia de la Unión Europea (TJUE) sobre protección de datos, focalizándose en las resoluciones adoptadas después de la entrada en vigor del RGPD. En efecto, las decisiones adoptadas por el TJUE permitirán determinar con mayor precisión el contenido del derecho a la protección de datos, en especial en lo que dice relación con conceptos tales como "responsable del tratamiento", "consentimiento del interesado", "interés legítimo del interesado" y, sustancialmente relevante para esta investigación doctoral, la "autoridad de control" en materia de protección de datos, siendo importante también para analizar la interpretación jurisdiccional sobre sus "competencias, funciones y poderes".

3. Revisar la regulación constitucional y legal de la protección de datos en Latinoamérica y Chile, identificando las normas que la regulan, su vigencia, contenido y ámbito de aplicación. En este sentido, se examinarán también los instrumentos jurídicos internacionales (tratados, convenios, declaraciones, recomendaciones, entre otros) que promuevan la configuración de criterios comunes para la regulación de la protección de datos en la región. Igualmente, se revisarán las Cartas Políticas Latinoamericanas, para determinar la existencia o no de un estándar normativo, y lo mismo se hará con las leyes sobre protección de datos, con el propósito de reconocer aspectos regulatorios comunes en cada uno de los países de la región.

4. Analizar y sistematizar los modelos de agencias reguladoras en materia de protección de datos europeas y latinoamericanas, identificando sus principales características. Este objetivo constituye uno de los propósitos centrales de esta investigación doctoral; para alcanzarlo, se realizará una revisión de las entidades que regulan la protección de datos a nivel de Unión Europea (UE) y Latinoamérica, analizando cuáles son los estándares o criterios comunes sobre los que se estructuran, si tienen independencia o no de los órganos de gobierno y cómo se expresa dicha independencia o autonomía, si son entidades unipersonales o colegidas, o si tienen o no facultades sancionadoras. De igual forma, se revisará en la experiencia comparada si las entidades de control se abocan exclusivamente a la regulación y promoción de la protección de datos o además asumen la garantía del derecho de acceso a la información pública, y si en uno u otro caso existen o no mecanismos institucionales de coordinación.

5. Analizar críticamente el proyecto de ley actualmente en tramitación en Chile, que regula la protección de datos y propone la configuración de una Autoridad de Control en la materia. Con este propósito se hará una revisión histórica de la ley N° 19.628 sobre Protección a la Vida Privada, sus orígenes, los cambios introducidos durante su tramitación legislativa, así como las modificaciones que ha tenido con posterioridad a su entrada en vigor. Igualmente se revisará acuciosamente el proyecto de ley que propone una nueva institucionalidad para la protección de datos en Chile, haciendo una

revisión de las entidades regulatorias existentes en la Administración Pública Chilena, sistematizando sus elementos de configuración, esto es, si son entidades autónomas, descentralizadas o centralizadas, si se estructuran como entidades colegiadas o unipersonales y, si estas autoridades son designadas por el ejecutivo de manera directa o a través de la interacción con otros poderes del Estado, como el Congreso Nacional, o si son agencias especializadas con foco o no en un determinado sector económico a regular, entre otros criterios de sistematización.

Metodología

Para el desarrollo de esta investigación se utilizarán diversas metodologías, propias de la ciencia jurídica, al analizar la normativa, la jurisprudencia y la doctrina. Metodología comparada en el análisis sobre cómo en otros países se estructuran las entidades públicas que protegen, regulan y promueven la protección de datos de carácter personal como derecho fundamental. Se estudiarán además sus respectivas regulaciones jurídicas, tanto en el ámbito constitucional como legislativo, lo que significará recurrir también a la dogmática jurídica para analizar las fuentes del derecho a la protección de datos.

Se abordarán también los principios y derechos conexos que permiten la configuración de la protección de datos como un derecho fundamental, analizando con un método histórico su surgimiento tanto en la Europa continental, especialmente en España, así como en Latinoamérica y Chile.

De igual forma, el presente trabajo revisa y analiza la jurisprudencia del Tribunal de Justicia de la Unión Europea (TJUE), haciendo una síntesis y explicación de sus fallos desde la entrada en vigor del Reglamento General de Protección de Datos 2016/679, el 25 de mayo del año 2018 hasta el 20 de mayo de 2020.

Para la realización de todo este trabajo se hará una búsqueda y recolección de literatura jurídica y documentos de carácter doctrinario y normativo, revisando bases de datos tales como *Web of Science*, Scopus, Scielo, libros, capítulos de libros, revistas jurídicas, portales de agencias de protección de datos, así como búsquedas en la red, bibliotecas y librerías especializadas. Igualmente se revisarán informes legislativos emanados de entidades parlamentarias.

Finalmente, en relación con el estudio de la doctrina jurídica utilizada para el desarrollo de la presente investigación, se ha asistido a foros y conferencias de expertos en protección de datos, quienes han expuesto su visión y a quienes se ha consultado sobre los mecanismos de tutela de la protección de datos, en especial en lo que dice relación con la configuración y características de una Autoridad de Control en la materia[7].

En definitiva, lo que este trabajo pretende concluir es que para garantizar el derecho fundamental a la protección de datos de carácter personal en Chile se requiere de una institucionalidad que la regule y promueva. Para ello, es indispensable el establecimiento de

[7] Por ejemplo, la conferencia de José Luis Rodríguez Álvarez, exdirector de la Agencia Española de Protección de Datos en el cierre del Máster de Transparencia y Acceso a la Información Pública que impartió en la Universidad Complutense de Madrid el año 2020. Actualmente es el Presidente del Consejo de Transparencia y Buen Gobierno de España.

un mecanismo de garantía o tutela, concretamente de una Autoridad de Control, la que debe configurarse como una entidad de la administración pública, dotada de capacidades y poderes que le permitan cumplir su objetivo, contando con las partidas presupuestarias o recursos adecuados para ello.

Preguntas de la Investigación

A lo largo de esta investigación se pretenden responder los siguientes cuestionamientos:

- ¿Qué orígenes tiene la protección de datos en la Europa continental?

- ¿Cuál es la relación de la protección de datos con otros derechos fundamentales como la intimidad y la vida privada?

- ¿Qué regulación normativa tiene la protección de datos tanto en Latinoamérica como en Chile?

- ¿Se requiere una Autoridad de Control en materia de protección de datos para Chile?

- ¿La Autoridad de control debe ser una entidad dependiente o independiente del ejecutivo?

- ¿Bajo qué elementos se configura la dependencia o independencia de una Autoridad de Control?

- ¿Dicha entidad debe ser un órgano autónomo, descentralizado o centralizado inserto en la administración pública?

- ¿Esta Autoridad de Control debe configurarse como una autoridad colegiada o unipersonal?

- ¿La Autoridad de Control debe abocarse exclusivamente a la regulación de la protección de datos o debe asumir conjuntamente con ello, la regulación del derecho de acceso a la información pública?

Para responder a estas preguntas, el presente trabajo se estructura sobre cinco capítulos, a saber: Capítulo I, “La Protección de Datos como Derecho Fundamental”; Capítulo II, “La Tutela de la Protección de Datos y su Jurisprudencia ante el Tribunal de Justicia de la Unión Europea”; Capítulo III, “La Protección de Datos en América Latina”; Capítulo IV, La Autoridad de Control para la Protección de Datos y su Independencia”; y Capítulo V, “Hacia la Institucionalización de la Protección de Datos para Chile”. Finalmente, en el último apartado se desarrollan las conclusiones de esta investigación.

Capítulo Primero

En el capítulo primero se abordará la concepción de la protección de datos personales como derecho fundamental, los que tienen su arraigo en la dignidad del ser humano, ya que según lo planteado por la teoría kantiana, antes de los derechos está el individuo, la persona y su dignidad, siendo esta dignidad inherente a la personalidad del ser humano. En este mismo sentido se analizarán también los instrumentos jurídicos internacionales que dan sustento a los derechos fundamentales en la dignidad del ser humano, tanto a nivel europeo como americano, así como su establecimiento en las constituciones alemana, española y chilena entre otras.

Además, se estudiará la relación de la protección de datos con otros derechos, tales como la intimidad y la vida privada, defendiendo que son derechos diferentes, como se explicará a lo largo de este trabajo. En efecto, como señala Garzón, la intimidad "es el ámbito de los pensamientos de cada cual, de la formación de sus decisiones, de las dudas que se escapan a una clara formulación, de lo reprimido, de lo aún no expresado que quizás nunca lo será, no solo porque no se desea expresarlo si no porque es inexpresable"[8].

Así también, el Tribunal Constitucional español ha reconocido expresamente que el derecho fundamental a la intimidad no aporta por sí solo una protección suficiente frente a las realidades nuevas derivadas del progreso tecnológico, por lo que la Constitución, al establecer que la ley debe limitar el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos, pone de manifiesto la existencia de los riesgos asociados a ese progreso, encomendando al legislador el desarrollo de garantías, que también son, en sí mismas, un derecho o libertad fundamental[9].

Por su parte, como se verá, la vida privada ha tenido acogida en la jurisprudencia internacional como el Tribunal Europeo de Derechos Humanos y la Corte Interamericana de Derechos Humanos, que han concebido la vida privada como una serie de factores relacionados con la dignidad del individuo, incluyendo, por ejemplo, la capacidad para desarrollar la propia personalidad y aspiraciones, determinar la propia identidad y definir las propias relaciones personales; englobando aspectos de la identidad física y social, incluyendo el derecho a la autonomía personal, desarrollo personal y el derecho a establecer y desarrollar relaciones con otros seres humanos y con el mundo exterior[10].

Como es posible advertir, si bien existe esta relación entre protección de datos personales, intimidad y vida privada, en muchos casos la información o datos de un titular tendrían escasa relación con su intimidad y vida privada. Así, por ejemplo, la información de una persona afiliada a un sindicato, nada tiene que ver con su intimidad o vida privada, no obstante, el tratamiento de esta información afecta el derecho a la protección de datos, por cuanto dicha filiación es un dato personal.

---

[8] Garzón Valdés, E. (2015), "Lo íntimo, lo público y lo privado", en *Cuadernos de Transparencia*, n°6. Instituto de Investigaciones Jurídicas, Universidad Nacional Autónoma de México, p.15.

[9] Sentencia del Tribunal Constitucional de España 245/1993, de 20 de julio de 1993, reiterada en la Sentencia 58/2018, de 4 de junio de 2018.

[10] CIDH, Caso Artavia Murillo y Otros ("Fecundación in vitro") vs. Costa Rica, Sentencia de Fondo (Excepciones Preliminares, Fondo, Reparaciones y Costas), de 28 de noviembre de 2012, párr. 143.

Este capítulo se referirá también al surgimiento de la normativa continental europea de la protección de datos en Alemania y su posterior desarrollo en el viejo continente, especialmente en el caso español, revisando además la noción norteamericana del *privacy* y el abordaje general de la protección de datos en Colombia, Perú y México, para centrarse luego en la ley sobre protección a la vida privada en Chile[11], así como la regulación en esta ley de los denominados derechos ARCO, y el posterior reconocimiento constitucional el año 2018 del derecho a la protección de datos personales.

El capítulo primero además analizará los Principios de la Protección de Datos dispuestos por la Organización para la Cooperación y el Desarrollo Económico, OCDE[12], así como el contenido del Convenio 108 del Consejo de Europa, instrumento internacional jurídicamente vinculante que tiene por objeto garantizar aquellos derechos vinculados a la intimidad, especialmente en lo que respecta al tratamiento de datos de carácter personal, consagrando internacionalmente el concepto de "protección de datos" como la protección o tutela jurídica de las personas con respecto al tratamiento automatizado de datos personales relativos al interesado, para luego analizar su posterior proceso de actualización.

Seguidamente se hace una revisión de los contenidos de la Directiva 95/46 y del Reglamento General de Protección de Datos Personales de la Unión Europea N° 2016/679[13] (RGPD a partir de ahora), para finalizar con una revisión del desarrollo legislativo de la Protección de Datos Personales en España con la vigente Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales.

Capítulo Segundo

El Capítulo segundo se refiere a los mecanismos de tutela de la protección de datos en el ámbito jurisdiccional, así como a los procedimientos administrativos contemplados en la esfera europea, específicamente se revisarán como mecanismos de tutela el derecho para presentar reclamaciones ante la respectiva autoridad de control, previstas en el RGPD, y la vía jurisdiccional o la tutela judicial efectiva, analizando la jurisprudencia del Tribunal de Justicia de la Unión Europea TJUE, desde la entrada en vigencia del Reglamento General de Protección de Datos 679/2016, el 25 de mayo del año 2018.

Se analizará que a diferencia de lo que ocurre en Chile, en el ámbito europeo, todo titular de datos de carácter personal o interesado tiene derecho a recurrir ante una autoridad de control, especialmente en el Estado miembro en el que tenga su residencia habitual, trabaje o se sitúe en el territorio del lugar donde se haya producido la infracción al Reglamento, pudiendo entablar una acción judicial o recurso ante las autoridades jurisdiccionales de los Estados miembros, de conformidad a su respectiva legislación. En definitiva, se verá que el interesado está facultado o tiene derecho a denunciar ante la autoridad de control[14], interponer recursos

[11] Ley N° 19.628.

[12] Ver en: https://www.oecd.org/sti/ieconomy/15590267.pdf

[13] Ver: https://www.boe.es/doue/2016/119/L00001-00088.pdf

[14] Puente Escobar, A. (2008), "La Agencia Española de Protección de Datos como garante del derecho fundamental a la protección de datos de carácter personal", *Azpilcueta*, n°20, pp.13-41.

judiciales ante el órgano jurisdiccional competente y recurrir a mecanismos de resolución extrajudicial de conflictos.

Así entonces, se examinará cómo la tutela judicial efectiva evolucionó desde sus orígenes en que era concebida como un derecho accesorio o complementario a otros, a ser un derecho fundamental reconocido en el artículo 8 de la Carta de los Derechos Fundamentales de la Unión Europea (CDFUE)[15], vinculado al derecho de protección de datos de carácter personal, regulado en el RGPD 2016/679, que ha ampliado el contenido y alcance de dicha tutela, en relación a la regulación que inicialmente estaba prevista en la Directiva 95/46/CE y que fue derogada por el citado RGPD, donde la influencia de la jurisprudencia del TJUE ha sido fundamental.

Este capítulo explicará y analizará el aporte del TJUE a través de la interpretación y resolución de las contiendas sometidas a su conocimiento en materias relacionadas con la divulgación de datos personales, la independencia de las autoridades de control en protección de datos, sus competencias y funciones, definición y alcance del término "datos personales", responsable del tratamiento de datos y delimitación de los derechos del interesado entre otros contenidos. Los fallos que se analizarán comprenden el periodo que va entre el 25 de mayo de 2018, fecha en la que entra en vigor el Reglamento General de Protección de Datos RGPD 2016/679, hasta mayo del año 2020.

Capítulo Tercero

En este capítulo se revisará el desarrollo de la protección de datos a nivel latinoamericano, además de una revisión de la regulación en protección de datos de los Estados Unidos de Norteamérica. Más concretamente la del Estado de California, la que entró en vigor el primero de enero del año 2020. Asimismo, se analizará la normativa iberoamericana existente, radicada fundamentalmente en instrumentos de *soft law*, fuertemente influenciados por el RGPD de la UE, como los recientes Principios de Datos Personales de la Organización de Estados Americanos, OEA[16] y de la Red Iberoamericana de Protección de Datos[17].

Se distinguirán los dos grandes modelos en protección de datos, el estadounidense y el europeo. Aunque existe un tercer tipo, que autores como Villegas Carrasquilla han denominado el modelo latinoamericano, y que se sustenta en el derecho fundamental de *habeas data*, que además de ser un derecho fundamental, es una acción de protección de la que gozan los titulares de los datos frente al tratamiento indebido o ilegal de los mismos, alojados en archivos de entidades tanto públicas como privadas[18]. Latinoamérica se diferencia del modelo europeo, fundamentalmente porque no existe una norma, tratado o instrumento multilateral (aparte de

[15] Ver: https://www.europarl.europa.eu/charter/pdf/text_es.pdf

[16] Ver: http://www.oas.org/es/sla/cji/docs/CJI-RES_266_XCVIII-21.pdf

[17] Ver: https://www.redipd.org/es/documentos/estandares-iberoamericanos

[18] Villegas Carrasquilla, L. (2012), "Protección de datos personales en América Latina: retención y tratamiento de datos personales en el mundo de Internet", en *Hacia una Internet Libre de Censura, Propuesta de América Latina, Facultad de Derecho, Centro de Estudios en Libertad de Expresión y Acceso a la Información*, compilador Eduardo Bertoni, Buenos Aires, p.130

las regulaciones iberoamericanas de *soft law*, ya señaladas) de carácter general que regule la protección de datos de carácter personal.

En este capítulo se revisará cómo diecinueve constituciones latinoamericanas regulan la protección de datos y se podrá apreciar que algunas consagran el hábeas data equiparándolo al derecho de la protección de datos personales, sin considerar que una cosa es el derecho a la protección de datos o autodeterminación informativa, que permite a su titular disponer de la información que le es propia, y otra, es el instrumento o recurso para tutelar o resguardar tal derecho accionando ante los tribunales de justicia.

Por otra parte, luego de revisar la regulación constitucional, se analizará la legislación sobre protección de datos existente en los países latinoamericanos, donde si bien existe diversidad en la profundidad y sistematización de las distintas leyes, es posible distinguir ciertos estándares comunes como: la definición de términos tales como "datos personales" y "datos sensibles"; los principios en que debe sustentarse el tratamiento de datos; los derechos de los titulares de los datos; la transferencia de datos; la autoridad de control en la materia; y la acción o procedimiento de tutela, así como las sanciones a que se verán expuestas las entidades públicas y privadas que no cumplan con sus disposiciones. Además, se constatará que en aquellos países que no tienen una regulación específica sobre protección de datos esta materia será abordada indirectamente por la legislación sobre transparencia y acceso a la información pública.

Capítulo Cuarto

En este capítulo se revisará cómo el RGPD establece la importancia de las autoridades de control para la promoción, fiscalización y control del tratamiento de datos de carácter personal, y luego, se analiza la configuración de las agencias de control en materia de protección de datos, tanto en el contexto europeo como latinoamericano, revisando también la situación de los países de la OCDE y las características que estas instituciones tienen en su conformación, es decir, si asumen exclusivamente la protección de datos o además conjuntamente regulan el acceso a la información pública y la transparencia, si son unipersonales o colegidas, si son autónomas o independientes o dependen de algún ministerio u otra entidad pública, o si tienen reconocimiento constitucional o legal, y si su alcance afecta al sector público, privado o a ambos, entre otras consideraciones. En el ámbito europeo para esta revisión se consideraron 27 países, que son los que integran la Unión Europea y que cuentan con agencias encargadas para la protección de datos, además de Gran Bretaña que recientemente ha abandonado la UE. Igualmente se revisarán las entidades de los países de la *OCDE*, haciendo una agrupación por los países europeos, americanos, oceánicos y asiáticos que integran dicho bloque. Además, se revisarán los países miembros de la Red Iberoamericana de Protección de Datos, bloque del cual forman parte tanto España como Chile.

De igual modo se revisará como el RGPD regula la Autoridad de Control analizando sus competencias, funciones y poderes, así como el rol que esta autoridad tiene en el tratamiento internacional y transfronterizo de datos personales.

A continuación, se analizarán las reformulaciones que la Ley 3/2018 sobre Protección de Datos y Garantías de Derechos Digitales (LOPDGDD) ha realizado sobre la estructura y funcionamiento de la Agencia Española de Protección de Datos, para finalizar con el análisis de la independencia y cómo esta incide en la estructuración de las agencias y autoridades de control para protección de datos, independencia que constituye un elemento fundamental en su configuración.

Finalmente, se revisarán los principios sobre mejores prácticas para la gobernanza de los reguladores o agencias independientes establecidos por la OCDE[19], que son lineamientos para fortalecer su diseño institucional y que, por tanto, buscan mejorar su desempeño, entendiendo que la Autoridad de Control en materia de protección de datos debe contar con los elementos necesarios para ejercer sus funciones.

Capítulo Quinto

Este capítulo final de la investigación doctoral se centra en la génesis y posterior desarrollo de la protección de datos en Chile, para avanzar hacia una institucionalización que la regule y promueva. En una primera parte se expone la regulación constitucional en materia de privacidad y protección a la vida privada en las diferentes Cartas Políticas chilenas, desde el Reglamento Constitucional de 1812 hasta la aún vigente Constitución chilena de 1980, la que está llegando a sus últimos meses de vigencia considerando el momento constituyente por el que atraviesa el país, y que el año 2018 incorporó en el catálogo de garantías constitucionales el derecho fundamental de la protección de datos personales.

A continuación, se analizará la historia de la ley sobre protección a la vida privada N° 19.628[20], donde se abordará su formulación en el año 1993 y de qué forma sus objetivos o propósitos iniciales, durante su extensa tramitación legislativa (la ley entró en vigor en el año 1999) fueron variando desde su presentación, donde se buscaba dar una adecuada protección al derecho a la privacidad de las personas ante eventuales intromisiones ilegítimas, estableciendo instrumentos de tutela que permitieran a las personas una efectiva protección de sus vidas privadas frente a los atropellos o amenazas de que pudieran ser objeto en el ejercicio de este derecho. Igualmente se revisarán las distintas modificaciones que esta legislación ha tenido y cuáles han sido los diferentes proyectos de ley que se han presentado y que no han continuado su tramitación legislativa, todos ellos vinculados con la protección de datos de carácter personal.

Luego, se estudiarán los principales aspectos del actual proyecto de ley que se encuentra en tramitación en el Senado chileno y que apuesta por un cambio sustancial en la regulación de la protección de datos, por cuanto su contenido incluye el establecimiento de una nueva institucionalidad, en concordancia con las tendencias regulatorias a nivel global. En efecto,

[19] Ver: https://www.oecd-ilibrary.org/governance/the-governance-of-regulators/chapter-3-decision-making-and-governing-body-structure-for-independent-regulators_9789264209015-8-en consulta efectuada el 24de junio de 2020.

20 Ver en: HLD_6814_37a6259cc0c1dae299a7866489dff0bd.pdf (bcn.cl) consulta realizada el 06 de enero 2021.

este proyecto incorpora la existencia de una Autoridad de Control en Protección de Datos, introduciendo también una serie de obligaciones a los responsables de datos coincidentes con el cambio de paradigma experimentado ya a nivel global en el Reglamento General de Protección de Datos (RGPD) de la Unión Europea. El proyecto actualmente en tramitación asume la protección de datos como un derecho fundamental, reconfigura los principios de la protección de datos, tales como el de licitud, finalidad, proporcionalidad y consentimiento. Además, consagra un nuevo procedimiento del titular de los datos para salvaguardar sus derechos, en lo que respecta al acceso, rectificación, cancelación y oposición, así como propone por vez primera en el sistema chileno la regulación de los datos biométricos. Del mismo modo, la legislación que se propone regula el tratamiento de los datos personales realizados por entidades privadas, pretendiendo corregir uno de los principales déficits de la legislación aún vigente, que solo se refiere al tratamiento de datos realizados por entidades públicas.

Se revisará además la propuesta de creación de una nueva institucionalidad de control, encargada de velar por el efectivo cumplimiento de la regulación en protección de datos, con funciones normativas, fiscalizadoras y sancionatorias. Siendo este uno de los principales puntos de discusión durante su tramitación, especialmente respecto a la naturaleza y rol del organismo en ciernes.

Finaliza este capítulo abordando el tipo de independencia o autonomía que debe tener la autoridad de control, para lo cual se revisarán las entidades con funciones de control, que siguiendo la experiencia comparada, se denominarán omnicomprensivamente, agencias reguladoras independientes y entre las cuales, en el sistema chileno, se distinguirán entre las Superintendencias, Órganos Constitucionalmente Autónomos y Entidades Colegiadas, ello con el objeto de tener un panorama general en lo relativo a sus niveles de independencia y autonomía, especialmente en lo referente a si la designación de su titular es exclusiva del poder ejecutivo, intervienen otros poderes del Estado o existe algún otro sistema público y transparente de concursabilidad. También, de las veintidós entidades estudiadas, se analizará si son órganos unipersonales o colegiados y si deberán regular o no de manera exclusiva la protección de datos, considerando que actualmente el proyecto que está en tramitación en el Senado le asigna la calidad de órgano de control en materia de protección de datos al Consejo para la Transparencia, lo que supondría tener una entidad con funciones mixtas, que además de regular la protección de datos se aboque al derecho de acceso a la información pública.

OBJECT, METHODOLOGY AND STRUCTURE

In Chile, Privacy Law No. 19,628[21] was issued in 1999, which, despite its name, specifically regulates the protection of personal data. This pioneering legislation in Latin America has become outdated and with little operability, not only due to the vertiginous nature of the transformations and technological changes that have occurred since it came into force, such as big data, social networks or artificial intelligence, but also due to the absence in said legislation of an entity that regulates and promotes the protection of personal data as a fundamental right.

At the constitutional level in Chile, unlike other countries in the region, it was not until 2018 that the protection of personal data was recognized as a fundamental right, a recognition that, however, has not promoted the indispensable legislative rule on the matter[22].

Since 2017, a bill that regulates the protection and management of personal data is being processed in the Chilean National Congress[23], that also creates an agency or entity in charge of its regulation. This bill has had a slow pace in Congress, still remaining in its initial constitutional stage, without significant progress in sight due to the current global context of the pandemic, thus everything indicates that this transcendental discussion will be postponed and addressed by a new government and congress, because in November of year 2021 there will be presidential and parliamentary elections.

Added to the above is the political and social context that Chile is going through, which has led to a unique constitutional process in its history and implies the development of a new constitutional text through a Constitutional Convention made up of 155 conventional constituents, who were elected on May 15 and 16, with gender parity (78 men and 77 women), seats for native people (17 seats reserved for representatives of the different indigenous ethnic groups) [24] and who have a total term of one year from their installation, on July 4 of this year 2021, to draft a new Charter, which must then be approved by the public through a ratifying plebiscite[25].

---

[21] Accesible at: https://www.bcn.cl/leychile/navegar?idNorma=141599, accessed on May 24, 2021.

[22] On June 16, 2018, law No. 21,096 was published in the Official Gazette, which establishes the protection of personal data as a constitutional guarantee, in number 4 of article 19 of the Chilean Constitution. Accesible at: Ley-21096 16-Jun-2018 Ministerio Secretaría General de la Presidencia - Ley Chile - Biblioteca del Congreso Nacional (Bcn.Cl) Accessed on May 24, 2021.

[23] Accessible at : https://www.camara.cl/legislacion/ProyectosDeLey/tramitacion.aspx?prmID=11661&prmBoletin=11144-07. Accessed on May 24, 2021.

[24] Accessible on: https://www.senado.cl/conozca-de-que-distritos-provendran-los-17-escanos-reservados-para/senado/2020-12-29/153330.html, accessed on May 24, 2021.

[25] Ver en: https://www.bcn.cl/procesoconstituyente/cronograma consulta realizada el 24 de mayo de 2021.

Although these circumstances imply a delay in the reconfiguration of a new institutional framework for data protection; at the same time they represent an opportunity to make the protection of personal data more valid and effective because the new Constitution must restructure rights already established, as well as incorporate new fundamental rights, with their respective instruments of protection or guarantee, being the case of data protection one of them, with the establishment of their respective control Agency.

For its part, Spain has for several decades now had an institutional framework that is in charge of data protection, through the Spanish Data Protection Agency[26], which is established as a benchmark in the matter and whose development and experiences are transformed in a role model not only for Chile, but also for all Latin America.

General Objective

The general objective of the doctoral research presented here is to propose the bases for the establishment of a Control Agency in matters of data protection for Chile, mainly taking as a reference the comparative European experience and especially Spain's experience with the Protection Agency of Data (AEPD) of that country, as well as the Latin American experience, especially with the entry into force of the new laws in Brazil and Ecuador, which will allow institutionalizing the protection of personal data in Chile. This thesis will comparatively analyze the entities in charge of regulating data protection in different countries and the criteria on which a regulatory agency must be configured.

Specific Objectives

In order to reach this general objective, the following specific objectives are proposed:

1. Analyze the protection of personal data as a fundamental right, from its origins in continental Europe, first resorting to the right to privacy (the right to be left alone or in peace) that arises in the United States, until its most recent regulation via the European Regulation for the Protection of Personal Data (RGPD) 2016/679. In the same manner, their relationship between privacy and intimacy will be analyzed, understanding that they are similar but diverse rights. In this sense, I seek to determine what is the content and scope of data protection, to then verify whether or not these rights imply a limit so that the data or information of an individual cannot be processed without their consent, or if they also include the power of their owner to freely dispose of them, controlling their disposal or even pursuing their data if necessary.

   I will also study whether there is a common relationship or link between data protection and the right of access to public information.

[26] https://www.aepd.es/es

Likewise, the so-called ARCO rights (Access, Rectification, Cancellation and Opposition) will be examined, to which it will be necessary to add the right to be forgotten digitaly and the right to data portability, incorporated in the RGPD.

Revisar y sistematizar la jurisprudencia del Tribunal de Justicia de la Unión Europea (TJUE) sobre protección de datos, focalizándose en las resoluciones adoptadas después de la entrada en vigor del RGPD. En efecto, las decisiones adoptadas por el TJUE permitirán determinar con mayor precisión el contenido del derecho a la protección de datos, en especial en lo que dice relación con conceptos tales como "responsable del tratamiento", "consentimiento del interesado", "interés legítimo del interesado" y, sustancialmente relevante para esta investigación doctoral, la "autoridad de control" en materia de protección de datos, siendo importante también para analizar la interpretación jurisdiccional sobre sus "competencias, funciones y poderes".

2. Review the constitutional and laws of data protection in Latin America and Chile, identifying the rules that regulate theses rights, their validity, content and scope of application. In this sense, international legal instruments (treaties, conventions, declarations, recommendations, among others) that promote the configuration of common criteria for the regulation of data protection in the region will also be examined. Likewise, the Latin American Political Letters will be reviewed to determine the existence or not of a regulatory standard, and the same will be done with the laws on data protection, with the purpose of recognizing common regulatory aspects in each of the countries of the region.

3. Analyze and systematize the models of regulatory agencies in matters of European and Latin American data protection, identifying their main characteristics. This objective constitutes one of the central purposes of this doctoral research. To achieve the latter, a review of the entities that regulate data protection at the level of the European Union (EU) and Latin America will be carried out, analyzing what are the common standards or criteria on which they are structured, whether or not they have independence from the bodies of government and how said independence or autonomy is expressed, whether they are sole proprietorships or collegiate entities, or whether or not they have sanctioning powers. In the same way, the comparative experience will review whether the control entities focus exclusively on the regulation and promotion of data protection or also assume the guarantee of the right of access to public information, and if in one case or another there are or not institutional coordination mechanisms.

4. Critically analyze the bill currently being processed in Chile, which regulates data protection and proposes the configuration of a Control Agency on the matter. For this purpose, a historical review will be made of Law No. 19,628 on the Protection of Private Life, its origins, the reforms introduced during its legislative process, as well as the modifications that it has had after its entry into force. Likewise, the bill that proposes a new institutional framework for data protection in Chile will be thoroughly

reviesed, making a review of the existing regulatory entities in the Chilean Public Administration, systematizing their configuration items, that is, if they are autonomous, decentralized or centralized entities, if they are structured as collegiate or unipersonal entities and if these authorities are appointed by the executive branch directly or through interaction with other branches of the State, such as the National Congress, or if they are specialized agencies with a focus or not on a determined economic sector to regulate, among other systematization criteria.

Methodology

For the development of this research, different methodology will be used, mainly a comparative analysis of how public entities are structured in other countries to regulate and promote the protection of personal data as a fundamental right. Their respective legal regulations will also be studied, both in the constitutional and legislative fields, which will also mean resorting to legal dogmatics to analyze the sources of the right to data protection.

The principles and related rights that allow the configuration of data protection as a fundamental right will also be addressed, analyzing its emergence both in continental Europe, especially in Spain, as well as in Latin America and Chile.

Similarly, this work reviews and analyzes the jurisprudence of the Court of Justice of the European Union (CJEU), providing a synthesis and explanation of their rulings since the entry into force of the General Data Protection Regulation 2016/679, on 25 May 2018.

To carry out all this work, a search and collection of legal literature and doctrinal and normative documents will be carried out, reviewing databases such as Web of Science, Scopus, Scielo, books, book chapters, as well as searches on the web, libraries and specialized bookstores. Likewise, legislative reports emanating from parliamentary entities will be reviewed

Finally, in relation to the method used for this research, there is the attendance to forums and conferences of experts in data protection, who have presented their vision and have been consulted on the mechanisms of protection of data protection, especially in relation to the configuration and characteristics of a Control Agency in the matter[27].

Ultimately, what this work intends to conclude is that in order to guarantee the fundamental right to the protection of personal data in Chile, an institutional framework is required to regulate and promote this matter. Hence, it is essential to establish a guarantee or guardianship mechanism, specifically a Control Agency, which must be configured as an entity of the public administration, endowed with capacities and powers to fulfill its objective, counting on the budgetary items or adequate resources for puirsing theses objectives.

[27] For example, the conference given by José Luis Rodríguez Álvarez, former director of the Spanish Agency for Data Protection at the closing of the Master's Degree in Transparency and Access to Public Information. Mr. Rodríguez is a lecturer at the Complutense University of Madrid in 2020.

Research Questions

Throughout this research, the main intention is to answer the following questions:

- What origins does data protection have in continental Europe?

- What is the relationship between data protection and other fundamental rights such as privacy and private life?

- What normative regulation does data protection have in both Latin America and Chile?

- Is a Data Protection Control Agency required for Chile?

- Should the Control Authority be a dependent or independent entity of the executive?

- Under what elements is the dependence or independence of a Control Agency configured?

- Should this agency be an autonomous, decentralized or centralized body inserted in the public administration?

- Should this Control Agency be configured as a collegiate or unipersonal authority?

- Should the Control Agency focus exclusively on the regulation of data protection or should it jointly assume the regulation of the right of access to public information?

To answer these questions, this thesis is structured around five chapters, namely: Chapter I, "Data Protection as a Fundamental Right"; Chapter II, "The Protection of Data Protection and its Case Law before the Court of Justice of the European Union"; Chapter III "Data Protection in Latin America", Chapter IV The Control Agency for Data Protection and its Independence"; and Chapter V "Towards the Institutionalization of Data Protection for Chile". Finally, in the last section the conclusions of this doctoral research are rendered.

Chapter One

In the first chapter, the conception of the protection of personal data as a fundamental right will be addressed. These rights are rooted in the dignity of the human being, since, according to the Kantian theory, before rights comes the individual, the person and their dignity, this dignity being inherent to the personality of the human being. In this same sense, the international legal instruments that support fundamental rights in the dignity of the human being, both at the European and American levels, as well as their establishment in the German, Spanish and Chilean constitutions, among others, will also be analyze.

In addition, the relationship of data protection with other rights will be studied, such as privacy and private life, defending that they are different rights, as will be explained throughout this work. Indeed, as Garzón points out, intimacy "is the sphere of each individual's thoughts, of the formation of their decisions, of the doubts that escape a clear formulation, of the repressed, of the not yet expressed that perhaps never will be, not only because you do not want to express it but because it is inexpressible" [28].

[28] Garzón Valdés, E. (2015), "Lo íntimo, lo público y lo privado", en *Cuadernos de Transparencia*, n°6. Instituto de Investigaciones Jurídicas, Universidad Nacional Autónoma de México, p.15.

Likewise, the Spanish Constitutional Court has expressly recognized that the fundamental right to privacy does not by itself provide sufficient protection against new realities derived from technological progress, which is why the Constitution, by establishing that the law must limit the use of information technology to guarantee honor, personal and family privacy of citizens and the full exercise of their rights, highlights the existence of the risks associated with this progress, entrusting the legislator with the development of guarantees, which are also, in themselves, a fundamental right or freedom[29].

For its part, as will be seen, private life has been received in international case law, such as the European Court of Human Rights and the Inter-American Court of Human Rights, which have conceived private life as a series of factors related to the dignity of the individual, including, for example, the ability to develop one's own personality and aspirations, determine one's identity, and define one's personal relationships; encompassing aspects of physical and social identity, including the right to personal autonomy, personal development and the right to establish and develop relationships with other human beings and with the external world[30].

As it is possible to notice, although there is a relationship between protection of personal data, privacy and private life, in many cases the information or data of a holder would have little relationship with their privacy and private life. Thus, for example, the information of a person affiliated with a union has nothing to do with their privacy or private life, however, the treatment of this information affects the right to data protection, since said affiliation is a piece of personal information.

This chapter will also refer to the emergence of continental European data protection regulations in Germany and its subsequent development in the old continent, especially in the Spanish case, also reviewing the North American notion of privacy and the general approach to data protection. in Colombia, Peru and Mexico, to then focus on the law on protection of private life in Chile[31],, as well as the regulation in this law of the so-called ARCO rights, and the subsequent constitutional recognition in 2018 of the right to data protection personal.

The first chapter will also analyze the Data Protection Principles established by the Organization for Economic Cooperation and Development, OECD**[32]**, as well as the content of Convention 108 of the Council of Europe, a legally binding international instrument that aims to guarantee those related rights. to privacy, especially with regard to the processing of personal data, internationally enshrining the concept of "data protection" as the protection or legal guardianship of people with respect to the automated processing of personal data relating to the interested party, and then analyze its subsequent update process.

Next, a review is made of the contents of Directive 95/46 and the General Regulation of Personal Data Protection of the European Union No. 2016/679[33] (“RGPD”), to end with a review of the legislative development of the Protection of Personal Data in Spain with the

---

[29] Sentencia del Tribunal Constitucional de España 245/1993, de 20 de julio de 1993, reiterada en la Sentencia 58/2018, de 4 de junio de 2018.

[30] CIDH, Caso Artavia Murillo y Otros (“Fecundación in vitro”) vs. Costa Rica, Sentencia de Fondo (Excepciones Preliminares, Fondo, Reparaciones y Costas), de 28 de noviembre de 2012, párr. 143.

[31] Law N° 19.628.

[32] Accessible at: https://www.oecd.org/sti/ieconomy/15590267.pdf

33 Accessible at: https://www.boe.es/doue/2016/119/L00001-00088.pdf

current Organic Law 3/2018, of December 5, on the Protection of Personal Data and Guarantee of Digital Rights.

Second Chapter

The second chapter refers to the mechanisms of enforcement of data protection in the jurisdictional field, as well as the administrative procedures contemplated in the European sphere, specifically the right to file claims before the respective control agency will be reviewed as enforcement mechanisms, provided by the RGPD, and the jurisdictional means or effective judicial protection, analyzing the case law of the Court of Justice of the European Union CJEU, since the entry into force of the General Data Protection Regulation 679/2016, on May 25, year 2018.

An analysis of what differently occurs in Chile will be provided, in the sense that at the European level, any owner of personal data or an interested party has the right to resort to a control agency, especially in the Member State in which they have their habitual residence, they work or they are located in the territory of the place where the infringement of the Regulation has occurred, being able to file a judicial action or appeal before the jurisdictional authorities of the Member States, in accordance with their respective legislation. Ultimately, the work will highlight the fact that the interested party is empowered or has the right to: File administrative actions before the control agency[34]; File judicial actions before the competent court and; Resorting to extrajudicial conflict resolution mechanisms.

Then an examination of how effective judicial protection has evolved from its origins when it was conceived as an accessory or complementary right to others, to being a fundamental right recognized in article 8 of the Charter of Fundamental Rights of the European Union (CDFUE) [35], linked to the right to personal data protection, regulated in the RGPD 2016/679, which has expanded the content and scope of said protection, in relation to the regulation that was initially provided for in Directive 95/46/CE and which was repealed by the aforementioned RGPD, where the influence of the CJEU case law has been fundamental.

This chapter will explain and analyze the contribution of the CJEU through the interpretation and resolution of the disputes submitted to them in matters related to the disclosure of personal data, the independence of the data protection control authorities, their powers and functions, definition and scope of the term "personal data", data controller and delimitation of the rights of the interested party, among other contents. The rulings that will be analyzed include the period between May 25, 2018, the date on which the General Data Protection Regulation RGPD 2016/679 enters into force, until May 2020.

34 Puente Escobar, A. (2008), "La Agencia Española de Protección de Datos como garante del derecho fundamental a la protección de datos de carácter personal", Azpilcueta, n°20, pp.13-41.

35 Accessible at: https://www.europarl.europa.eu/charter/pdf/text_es.pdf

Third Chapter

This chapter will review the development of data protection at the Latin American level, previously making a review of the US regulation on data protection, specifically that of the State of California, which came into force on January 1, 2020. Likewise, the existing Ibero-American regulations will be analyzed, fundamentally based on soft law instruments, strongly influenced by the EU RGPD, such as the recent Personal Data Principles of the Organization of American States, OAS and the Ibero-American Data Protection Network[36].

The communication from the Commission to the European Parliament and the Council of June 24, 2020[37], which gives an account of the implementation and effects that the application of the RGPD has had since its in force, on May 25, 2018, will also be reviewed. to distinguish in what way and to what depth the EU countries have adjusted their legislation to these standards or are in the process of doing so.

The two main models in data protection, American and European, will be distinguished. Although there is a third type, which authors such as Villegas Carrasquilla have coined as the Latin American model, and is based on the fundamental right of habeas data, that in addition to being a fundamental right, is a protection action enjoyed by the holders of the data, against the improper or illegal treatment thereof, housed in files of both public and private entities[38]. Latin America differs from the European model, fundamentally because there is no multilateral norm, treaty or instrument (apart from the Ibero-American soft law regulations, already mentioned) of a general nature that regulates the protection of personal data.

In this chapter, we will review how nineteen Latin American constitutions regulate data protection and it will be possible to confirm that some of them provide an habeas data, equating the same to the right to protect personal data, without considering that the right to data protection or informational self-determination allows its owner to manage the information that is his own, and another, is the instrument or resource to protect or enforce such right by taking action before the courts of justice.

On the other hand, after reviewing the constitutional regulation, the current legislation on data protection in Latin American countries will be analyzed. Even though there is diversity in the depth and systematization of the different laws, it is possible to distinguish certain common standards such as: the definition of terms such as "personal data" and "sensitive data"; the principles on which data processing must be based; the rights of the owners of the data; data transfer; the control agency in the matter; and the enforcement action or procedure, as well as the sanctions to which public and private entities that do not comply with its provisions will be exposed to. In addition, the research will verify that in those countries where there are no

[36] Accessible at: https://www.redipd.org/es/documentos/estandares-iberoamericanos

[37] Accessible at: https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:52020DC0264&from=ES

[38] Villegas Carrasquilla, L. (2012), "Protección de datos personales en América Latina: retención y tratamiento de datos personales en el mundo de Internet", en *Hacia una Internet Libre de Censura, Propuesta de América Latina, Facultad de Derecho, Centro de Estudios en Libertad de Expresión y Acceso a la Información*, compilador Eduardo Bertoni, Buenos Aires, p.130

specific regulations on data protection, this matter is indirectly addressed by the legislation on transparency and access to public information.

Chapter Four

In this chapter we will review how the RGPD establishes the importance of the control authorities for the promotion, inspection and control of the processing of personal data, and then, the configuration of the control agencies in terms of data protection is analyzed both in the European and Latin American context, also reviewing the situation of the OECD countries and the characteristics that these institutions have in their composition, that is, if they exclusively assume data protection or also jointly regulate access to public information and the transparency, if they are unipersonal or collegiate, if they are autonomous or independent or depend on a ministry or other public entity, or if they have constitutional or legal recognition, and if their scope affects the public, private or both sectors, among other considerations.

At the European level, for this review, 27 countries were considered, which are those that make up the European Union and that have agencies in charge of data protection, in addition to Great Britain, which has recently left the EU. Likewise, the entities of the OECD countries will be reviewed, making a grouping by the European, American, Oceanic and Asian countries that make up said block. In addition, the member countries of the Ibero-American Data Protection Network, a block of which both Spain and Chile are part, will be reviewed.

In the same way, a review on how the RGPD regulates the Control Authority is provided, analyzing its competences, functions and powers, as well as the role that this authority has in the international and cross-border processing of personal data.

Next, the reformulations that Law 3/2018 on Data Protection and Guarantees of Digital Rights (LOPDGDD) has carried out on the structure and operation of the Spanish Agency for Data Protection will be analyzed, to end with the analysis of independence and how this affects the structuring of the agencies and control authorities for data protection, independence that constitutes a fundamental element in its configuration.

Finally, the principles on best practices for the governance of regulators or independent agencies established by the OECD[39] will be reviewed, which are guidelines to strengthen their institutional design and, therefore, seek to improve their performance, understanding that the Control Agency in the matter of data protection must have the necessary elements to undertake its legal mandate.

[39] Ver:https://www.oecd-ilibrary.org/governance/the-governance-of-regulators/chapter-3-decision-making-and-governing-body-structure-for-independent-regulators_9789264209015-8-en consulta efectuada el 24de junio de 2020.

Chapter Five

This final chapter of the doctoral research focuses on the genesis and subsequent development of data protection in Chile to advance towards an institutionalization that regulates and promotes it. In the first part, the constitutional regulation on privacy and protection of private life is exposed in the different Chilean Political Letters, from the Constitutional Regulation of 1812 to the still current Chilean Constitution of 1980, which is reaching its last months of validity considering the constitutional moment that the country is going through, and that in 2018 the fundamental right to the protection of personal data was incorporated into the catalog of constitutional guarantees.

Next, the history of the law on protection of private life No. 19,628 will be analyzed, where its formulation in 1993 will be addressed and in which manner its objectives or initial purposes, during its extensive legislative process (the law entered into force in 1999) were varying from their presentation, where it was sought to give adequate protection to the right to privacy of people in the event of illegitimate interference, establishing enforcement means that would allow people an effective protection of their private lives against abuses or threats that could be the object in the use of this right. Likewise, the different modifications that this legislation has had and which have been the different bills presented and that have not continued their legislative processing will be reviewed, all of them related to the protection of personal data.

Then, the main aspects of the current bill that is being processed in the Chilean Senate will be studied and that is commitment to a substantial change in the regulation of data protection, since its content includes the establishment of a new institutionality, in accordance with regulatory trends at a global level. Indeed, this project incorporates the existence of a Data Protection Control Agency, also introducing a series of obligations to those responsible for data coinciding with the paradigm shift already experienced globally in the General Data Protection Regulation (RGPD) of the European Union. The project currently in process assumes data protection as a fundamental right, reconfigures the principles of data protection, such as legality, purpose, proportionality and consent. In addition, it establishes a new procedure for the owner of the data to safeguard their rights, with regard to access, rectification, cancellation and opposition; as well as proposing for the first time in the Chilean system the regulation of biometric data. In the same way, the proposed legislation regulates the processing of personal data carried out by private entities, seeking to correct one of the main deficits of the legislation still in force, which only refers to the processing of data carried out by public entities.

The proposal to create a new control institution will also be reviewed, in charge of ensuring effective compliance with data protection regulations, with regulatory, supervisory and sanctioning functions. The latter being one of the main points of discussion during its processing, especially regarding the nature and role of the budding organism.

We conclude this chapter by addressing the type of independence or autonomy that the control agency must have, for which the entities with control functions will be reviewed, that by following the comparative experience, will be called all-encompassing independent regulatory

agencies and among which, in the Chilean system, a distinction will be made between the Superintendencies, Constitutionally Autonomous Bodies and Collegiate Entities, in order to have a general overview regarding their levels of independence and autonomy, especially regarding whether the appointment of President is exclusive to the executive branch, other powers of the State intervene or there is some other public and transparent system of competition. Also, of the twenty-two entities studied, an analysis of whether they are unipersonal or collegiate bodies and whether or not they should exclusively regulate data protection will be rendered, considering that currently the project that is being processed in the Senate assigns it the quality of control body in terms of data protection to the Council for Transparency, which would mean having an entity with mixed functions, which, in addition to regulating data protection, addresses the right of access to public information.

CAPÍTULO I
LA PROTECCIÓN DE DATOS COMO DERECHO FUNDAMENTAL

La Dignidad Humana como sustento de los Derechos Fundamentales

Para el abordaje de la protección de datos personales como derecho fundamental (especialmente nuevo en el ordenamiento constitucional chileno) es preciso considerar que los derechos fundamentales tienen su sustento en la dignidad humana. Leopoldo Abad al referirse a la clasificación de los siete capítulos (dignidad, libertades, igualdad, solidaridad, ciudadanía, justicia y disposiciones generales) de la Carta de Derechos Fundamentales de la Unión Europea señala que "son muchas las opiniones vertidas sobre esta clasificación, no todas ellas positivas, pero si en algo podemos estar de acuerdo es en la necesaria interrelación de los derechos reconocidos en cada capítulo, partiendo de que la dignidad gravita y fundamenta el resto de los derechos"[40] En el caso de la protección de datos personales, parece claro que "emana" de la dignidad de la persona humana –no es un derecho ni de los animales, ni de las personas jurídicas- además que es un derecho que se encuentra estrechamente vinculado con otros derechos, como son el derecho a la intimidad, el respeto y protección a la vida privada y el derecho a la privacidad.

Como señala Manuel Sánchez de Diego Fernández de La Riva[41], "la aparición de nuevos derechos fundamentales y la evolución de los preceptos constitucionales es normal. Recordemos que los alemanes han construido el derecho a la intimidad a partir del derecho a la autodeterminación de la persona o «libre desenvolvimiento de su personalidad» (párrafo 1º del artículo 2 de la Ley Fundamental de Bonn de 1949). Por tanto, la propuesta de construcción de un derecho fundamental no es algo nuevo… Cuando la Constitución no formula directamente un derecho fundamental, sí es posible el reconocimiento del mismo a partir de una norma «adscripta». Norma que tiene una directa relación con la Constitución -debemos de entender que viene a desarrollar o completar algún precepto constitucional. Tal es el supuesto en nuestro país (España) del derecho a la protección de datos personales que cobra contenido con el desarrollo del artículo 18.4 de la Constitución en un primer momento por la Ley Orgánica de Regulación del Tratamiento Automatizado de Datos de carácter personal (LORTAD) de 1992 y posteriormente sustituida por la Ley de Protección de Datos Personales de 1999 (LOPD)", en la actualidad la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales, en adelante LOPDP y GDD.

---

[40] Abad Alcalá L. (2020). *Las libertades informativas en el ámbito internacional*. Dykinson. p.124

[41] Sánchez Diego Fernández de la Riva, M. "El derecho de acceso a la información pública", en Cotino Hueso, L. y Valero Torrijos, J. (Coordinadores) (2010), *"Administración Electrónica". La Ley 11/2007, de 22 de junio, de "acceso electrónico de los ciudadanos a los Servicios Públicos y los retos jurídicos del e-gobierno en España"*, Ed. Tirant lo Blanch, Valencia, pp. 325 a 348.

Aldunate[42] plantea tres opciones para definir la expresión de "derechos fundamentales": i) en un sentido general, y de hecho el más difundido, la citada expresión se usa para aludir a aquellos derechos de la persona que han recibido consagración positiva, en particular, a nivel constitucional; ii) otra postura identifica estos derechos como aquellos de los que es titular el hombre, no por graciosa concesión de las normas positivas, sino con anterioridad e independientemente de ellas y por el mero hecho de tal tratándose entonces de aquellos atributos vinculados directamente a la dignidad humana y que constituyen un conjunto limitado en su extensión solo a aquellos que son condición para la satisfacción de las necesidades inherentes a una vida digna; y iii) como tercera alternativa, se sugiere identificar esos "derechos fundamentales" como aquellos derechos subjetivos que corresponden universalmente a todos los seres humanos al poseer el *status* de personas con capacidad de obrar, de ser ciudadano.

En cualquier caso, antes de los derechos fundamentales está el individuo, su persona y dignidad. La noción de dignidad, del latín *"dignitas"*, que se traduce por valioso, hace referencia según Kant a un valor inherente al ser humano, por el hecho de ser tal, en cuanto individuo, dotado de libertad y racionalidad. La teoría kantiana postula a la dignidad como valor fundamental de la persona y de su personalidad, por lo que la dignidad se configura como principio legitimador de los denominados derechos de la personalidad.

Pero esta concepción kantiana de dignidad ha evolucionado, complejizándose, entendiéndola por una parte como una garantía negativa, esto es, derecho a no sufrir afectaciones o detrimentos, y por otra, como una garantía positiva, es decir, el derecho a disponer, esto es, a la autodeterminación de la persona. Lo que según Pérez Luño[43] constituye el pleno desarrollo de la personalidad. Por consiguiente, la dignidad es el fundamento de los derechos fundamentales que son expresiones y derivaciones de la dignidad para el desarrollo integral de la persona, por medio de los derechos que se han positivizado o normativizado.

Por lo anterior, diversos instrumentos jurídicos internacionales, así como Cartas Fundamentales, se han referido a la dignidad para sustentar los derechos fundamentales[44]. En relación con los instrumentos internacionales encontramos la Declaración de principios de la Organización Internacional del Trabajo OIT, también conocida como la Declaración de Filadelfia[45], que en lo que interesa dispone en el apartado II, letra a) "todos los seres humanos, sin distinción de raza, credo o sexo, tienen el derecho de perseguir su bienestar material, y su desarrollo espiritual en condiciones de libertad y dignidad, de seguridad económica y de igualdad de oportunidades…"

---

[42] Aldunate Lizana, E. (2008), *"Derechos Fundamentales"*, Santiago, Legal Publishing, p.47.

[43] Pérez Luños, A. E. (2010), *"Derechos Humanos, Estado de Derecho y Constitución"*, 10a Edición, Madrid, Tecnos, p.324.

[44] Es importante precisar que estamos equiparando la noción de derechos fundamentales con la de derechos humanos, aunque no son exactamente lo mismo. En términos generales se puede señalar que la diferencia entre derechos humanos y derechos fundamentales es que los derechos humanos son de carácter universal (protegen a todos los individuos), por lo tanto, no dependen de los Estados, y al tener alcance internacional van más allá de lo dispuesto en la Constitución o las leyes de un país, por lo que son de cumplimiento obligatorio. Por su parte, los derechos fundamentales son las garantías que aplican exclusivamente a los ciudadanos o residentes de un territorio determinado, su alcance es nacional y sus disposiciones y cumplimiento dependen del respectivo Estado.

[45] http://www.ilo.org/public/libdoc/ilo/1944/44B09_10_span.pdf

De igual forma el artículo 1° de la Declaración Universal de los Derechos Humanos de 1948[46] comienza reconociendo que "todos los seres humanos nacen y permanecen libres e iguales en dignidad y derechos.". Así también, el Pacto Internacional de Derechos Civiles y Políticos y el Pacto Internacional de Derechos Económicos, Sociales y Culturales, como las Convenciones internacionales sobre los derechos de los niños, de los trabajadores migrantes, como de las personas discapacitadas entre otros, han incorporado o referido a la dignidad en sus mensajes o articulado. Todo lo expuesto es demostración que, en el orden internacional, la dignidad se configura como un elemento esencial sobre el cual se sustentan los derechos fundamentales.

En el ámbito europeo, si bien durante algún tiempo la concepción de dignidad no se establece en términos explícitos, resulta inequívoca su presencia y relevancia. En efecto, ni en el Estatuto del Consejo de Europa de 1949, ni en el Convenio Europeo de Derechos Humanos de 1950, ni en la primera versión de la Carta Social Europea de 1961[47] se hace referencia expresa a la dignidad. En la Unión Europea, no es sino hasta la reforma del Tratado de Lisboa o Tratado de Funcionamiento de la Unión Europea, suscrito en el año 2007 (que entra en vigor en el 2009), que se incorpora la Carta de los Derechos Fundamentales de la Unión Europea[48] otorgándole una naturaleza jurídicamente vinculante, haciendo expresa mención a la dignidad. Así el art. 2° de dicho tratado dispone: "La Unión se fundamenta en los valores de respeto de la dignidad humana, libertad, democracia, igualdad, Estado de Derecho y respeto de los derechos humanos, incluidos los derechos de las personas pertenecientes a minorías."

También destaca el Tribunal Europeo de Derechos Humanos en el caso *"Tyrer vs. Reino Unido"*[49], relativo a los tratos inhumanos y degradantes, donde interpreta que un objetivo principal del Convenio Europeo de Derechos Humanos, es precisamente preservar y resguardar la dignidad humana, que no solo involucra el efecto físico y la gravedad de un castigo corporal, sino también "el trato de la persona como mero objeto por parte de la autoridad", estableciendo el tratamiento denigrante como lesión a la dignidad y a la integridad psíquica de la persona.

En el ámbito del derecho interno de los países, diversas constituciones se han referido en términos expresos a la dignidad humana, otorgándole un valor sustancial en la estructura de sus respectivos ordenamientos jurídicos. A modo de ejemplo, la Constitución Alemana de 1949, en su capítulo 1° se refiere a los derechos fundamentales y su protección, siendo precisamente el primero la dignidad humana. Luego, la reforma constitucional de 1990 reformuló la noción de dignidad al disponer: "La dignidad del hombre es sagrada y constituye deber de todas las autoridades del Estado su respeto y protección", pero mantuvo como primero el capítulo de los derechos fundamentales, encabezados por la dignidad humana.

La Constitución Española, influenciada por el constitucionalismo alemán, dispone en su art. 10.1 que: "La dignidad de la persona… es fundamento del orden político y de la paz social"

---

[46] http://www.ohchr.org/EN/UDHR/Documents/UDHR_Translations/spn.pdf.

[47] Sí se hace referencia en la versión revisada de 1997, con respecto al orden socio laboral, lo que denomina dignidad en el trabajo.

[48] Firmada solemnemente en Niza en el año 2000, señala en su preámbulo que la Unión Europea se funda sobre "el valor indivisible y universal de la dignidad humana", añadiendo luego en su art.1° que "la dignidad humana es inviolable y será respetada y protegida".

[49] Sentencia del Tribunal Europeo de Derechos Humanos del 25 de abril de 1978, N° de Recurso 5856/72.

estableciendo en su título primero la dignidad de la persona como fundamento del ordenamiento jurídico español.

> De igual forma la Constitución chilena establece en su artículo 1° inciso primero que: "Las personas nacen libres e iguales en dignidad y derechos.". Sobre este artículo conviene destacar aquí que el capítulo primero de la Constitución chilena, titulado "Bases de la Institucionalidad", contiene los principios e ideas matrices en las que se sustenta la unidad del ordenamiento jurídico chileno, no obstante, si bien existe una referencia expresa a la dignidad de las personas, esta no tiene un adecuado tratamiento en el establecimiento de los derechos fundamentales, reconocidos y tutelados en las denominadas garantías constitucionales. Actualmente Chile se encuentra en un proceso constituyente, el 25 de octubre del año 2020 se realizó el plebiscito que determinó avanzar en la elaboración de un nuevo texto constitucional que revisará los Derechos y Deberes constitucionales, establecidos en el Capítulo III de la Constitución vigente. Precisamente se trata de una modificación que ha sido planteada por diversos sectores jurídico-políticos en relación con el tratamiento que la actual Carta otorga a la dignidad humana, donde si bien la consagra en el artículo 1°, no la tutela o protege adecuadamente en el capítulo de las garantías constitucionales. En efecto, no hay disposición alguna que se refiera expresamente a la dignidad como derecho fundamental ni acción o recurso que la proteja.

Como se desprende de lo planteado por Pérez Luño[50], la dignidad es el sustento de los derechos fundamentales que permiten concretar y satisfacer las necesidades de la persona en el ámbito moral y es por esa relación que la doctrina clásica ha distinguido los derechos de la personalidad, tales como el derecho al honor, el derecho a la intimidad, el derecho al respeto y protección a la vida privada, la libertad de conciencia y más recientemente (especialmente en el caso chileno) el derecho a la protección de datos personales. Es decir, son derechos que el individuo tiene por él solo, pero también significativo hecho de ser tal. Es la dignidad, como señala Carrillo[51], el fundamento de los derechos personalísimos, lo que implica una doble garantía para la persona: una garantía negativa que asegura que no deberá ser objeto de intromisiones, y una garantía positiva, que permita la preservación de la intimidad como punto de apoyo para el pleno desarrollo de la personalidad del individuo.

Para la comprensión de la protección de datos personales como derecho fundamental, sustentado en la dignidad humana, resulta primordial analizar y entender el derecho a la intimidad, así como el derecho a la privacidad o al respeto y protección a la vida privada. En las siguientes líneas nos abocaremos al estudio de estos derechos de la personalidad intrínsecamente vinculados, que, aunque similares, tienen contenidos y alcances particulares y diferenciados.

---

[50] Pérez Luños, A. E. (2010), *"Derechos Humanos, Estado de Derecho y Constitución"*, 10ª Edición. Madrid, Tecnos, p.234.

[51] Carrillo, M. (2016), "Los ámbitos del derecho a la intimidad en la sociedad de la comunicación" en *Cuadernos y Debates* n° 248: El derecho a la privacidad en un nuevo entorno tecnológico, Madrid, Centro de Estudios Políticos y Constitucionales, p.24.

El Derecho a la Intimidad

La palabra "intimidad" tiene su antecedente latino en el vocablo "*intimus"* y el Diccionario de la Real Academia de la Lengua Española la define como "Zona espiritual íntima y reservada de una persona o de un grupo, especialmente de una familia"[52]. Por consiguiente, la intimidad se relaciona con el ámbito familiar y doméstico, ajeno al interés público, y, por lo tanto, vinculado a lo reservado.

Como señala José María Desantes[53], el sentido etimológico de intimidad nos comienza a abrir un camino para su definición. Íntimo procede de *intimus*, que es una variación filológica de *intumus*, forma superlativa del adverbio *intus*, dentro. Íntimo, es pues, aquello que está lo más adentro posible. No solo lo que está en el interior del hombre, sino lo que está en el "cogüelmo" mismo de su humanidad.

El término intimidad tiene concepciones diversas, por ejemplo, los italianos hablan de *riservatezza*, los franceses utilizan la expresión *vie pivée*, los alemanes se refieren al *privatspäre* y los países anglosajones utilizan el término *privacy*, si bien los conceptos de intimidad y de privacidad son diferentes, en el derecho anglosajón el derecho a la intimidad se traduce como *rigth to privacy.*

La jurisprudencia del Tribunal Constitucional alemán, en la sentencia que declaró como contrarias a la Ley Fundamental alemana o *Grundgesetz* algunas disposiciones de la Ley del Censo de 1982[54], recogió de la doctrina la denominada teoría de las tres esferas o círculos concéntricos[55], relacionada con el grado de afectación en el ámbito de los derechos de la personalidad garantizados en el artículo 2.1, en relación con la dignidad humana reconocida en el artículo 1.1, ambos de la Ley Fundamental alemana o *Grundgesetz*. Esta teoría establece la existencia de tres esferas; la primera, la esfera íntima *–Intimsphäre-*, se refiere a lo más secreto del individuo; la segunda, la esfera de lo privado *–Privatsphäre-*, similar al *privacy* anglosajona y al derecho a la intimidad español, en la cual se contienen la vida privada y las relaciones familiares y personales; por último, la esfera individual *–Individualshäre-*, que se refiere a los aspectos vinculados al honor y a la propia imagen. Así esta teoría plantea la existencia de tres círculos concéntricos en los que se desenvuelve el individuo, el de lo íntimo, el de lo privado y el de lo público.

El ordenamiento jurídico alemán no se refiere ni al *privacy* anglosajón ni a la intimidad como antecedentes o derechos relacionados con la protección de datos, sino que su vinculación se encuentra, como se ha señalado, en la dignidad humana y el libre ejercicio de la personalidad,

---

[52] Ver: https://dle.rae.es/intimidad?m=form

[53] Versión escrita de la exposición de José María Desantes, titulada *El Derecho Fundamental a la Intimidad*, en Seminario "El derecho a la intimidad y a la vida privada y los medios de comunicación social", realizado el 28 de agosto de 1991 en el Centro de Estudios Públicos, Santiago de Chile.

[54] Esta ley aprobada por el *Bundestag* o parlamento alemán instaba a los ciudadanos a contestar más de cien preguntas en el contexto del censo poblacional, algunos se negaron a responder, accionando el Estado contra ellos, generando las consecuencias derivadas de la judicatura constitucional de ese país que se señalan.

[55] Hubmann, H. (1967), "*Das Personlichkeitsrecht*", Colonia, 2° edición, pp.268 y ss.; Seidel, U. (1974), "*Datenbanken und Datenschutz*", Frankfurt, p.65.

conformando el derecho a la autodeterminación informativa.[56] La sentencia a la que se hace referencia dispone, en lo referente a la protección de datos personales, lo siguiente:

"En las condiciones de la elaboración moderna de datos, la protección del individuo contra la recogida, almacenamiento, utilización y difusión ilimitada de sus datos personales queda englobada en el derecho general de protección de la persona del artículo 2°, párrafo 1 en relación con el artículo 1° del párrafo 1 de la Ley Fundamental. El derecho constitucional garantiza en esta medida la facultad del individuo de determinar fundamentalmente por sí mismo la divulgación y utilización de los datos referentes a su persona"[57].

Por consiguiente, esta sentencia distingue o separa la protección de datos de la intimidad, el honor y la propia imagen, y enmarca en la protección a la dignidad las garantías establecidas para la tutela de los derechos fundamentales. La sentencia también, casi de manera clarividente, anticipa las complejidades que el desarrollo de la automatización, lo que hoy denominamos las tecnologías de la información, el *big data* o la inteligencia artificial, representan para resguardar la protección de los datos personales, lo que exige adecuados niveles de regulación. Señala la sentencia:

"Los procesos de decisión ya no se pueden retrotraer como antiguamente a registros y documentos compilados manualmente; antes bien, hoy en día gracias a la ayuda de la elaboración automática de datos, la información individual sobre las circunstancias personales u objetivas de una persona determinada o, en su caso determinable (…) son técnicamente hablando acumulables sin límite alguno y en cualquier momento se pueden recabar en cuestión de segundos, cualquiera que sea la distancia. Es más, esa información puede- especialmente en el montaje de sistemas integrados de información- refundirse con otras colecciones de datos en un perfil de personalidad parcial o ampliamente definido, sin que el interesado pueda controlar suficientemente su exactitud y su utilización. De este modo se han ensanchado en una medida hasta ahora desconocida las posibilidades de indagación e influencia susceptibles de incidir sobre la conducta del individuo, si quiera sea por la presión psicológica que supone el interés del público en aquella".

De manera más difusa el Tribunal Constitucional español dispone que la intimidad excluye las intromisiones de los demás en la esfera de la vida personal y familiar de los ciudadanos[58], no obstante reafirma la importancia del derecho a la intimidad al afirmar que "la intimidad personal y familiar reconocida en el artículo 18 de la Constitución Española (CE), y que implica la existencia de un ámbito propio y reservado frente a la acción y conocimiento de los demás, necesario según las pautas de nuestra cultura, para mantener una calidad mínima de la vida humana. Se muestran así esos derechos como personalísimos, ligados a la existencia del individuo"[59].

En la Constitución chilena, no existe una referencia explícita a la intimidad, en efecto el artículo 19, N°4 dispone "El respeto y protección a la vida privada y a la honra de la persona

[56] Recht auf informationelle selbstbestimmung.

[57] Traducción de Manuel Daranas, publicada en el Boletín de Jurisprudencia Constitucional n° 33, de las Cortes Generales, Madrid, 1984, pp. 126-170.

[58] Auto del Tribunal Constitucional 221/1990 (FJ3°).

[59] Sentencia del Tribunal Constitucional español 231/1988 de 2 de diciembre.

y su familia, y asimismo, la protección de sus datos personales. El tratamiento y protección de estos datos se efectuará en la forma y condiciones que determine la ley"[60].

A su turno, el artículo 19, N°5 establece: "La inviolabilidad del hogar y de toda forma de comunicación privada. El hogar solo puede allanarse y las comunicaciones y documentos privados interceptarse, abrirse o registrase en los casos y formas determinados por la ley".

Así entonces, la Constitución Política de la República de Chile, en su artículo 19, N°4, asegura a todas las personas el respeto y protección a la vida privada y pública y a la honra de la persona y de su familia, y de manera más reciente, a la protección de sus datos personales. Aunque el texto constitucional chileno englobe en un solo apartado el derecho a la honra y el derecho a las distintas esferas en que se desenvuelve la vida del hombre, se trata de derechos conceptual y efectivamente distintos. El propio contexto fundamental lo confirma. A continuación, el mismo artículo 19, N°4, se refiere al honor o la honra, dos perspectivas diferentes de un mismo derecho. En cambio, el artículo 19, N°5, alude claramente a la vida privada cuando asegura la inviolabilidad del hogar y de toda forma de comunicación privada. El hogar solo puede allanarse y las comunicaciones y documentos privados interceptarse, abrirse o registrarse en los casos y formas determinados por la ley. El derecho a la inviolabilidad del hogar, término más preciso y entrañable que el de domicilio y el derecho al secreto de las comunicaciones privadas y la correspondencia, no son otra cosa que instrumentos jurídicos externos de protección de la vida privada.

Diversos textos internacionales hacen referencia al derecho a la intimidad, aun cuando no utilicen el término expresamente si se refieren a la vida privada, a la familia, al domicilio o al honor, elementos todos relacionados con este núcleo de la personalidad; en efecto, la Declaración Universal de los Derechos Humanos de 1948[61], el Pacto de Derechos Civiles y Políticos de 1966[62], el Convenio de Roma o Convenio para la Protección de los Derechos Humanos y de las Libertades Fundamentales de 1950[63], se refieren a este derecho esencial en el núcleo de la personalidad.

De manera casi indiscutible la doctrina reconoce[64] el surgimiento del derecho a la intimidad como lo concebimos en la actualidad, con el artículo del año 1890 titulado "*The right to privacy*", en la publicación del *Harvard Law Review* de los autores Samuel Warren y Louis

[60] Con fecha 16 de junio de 2018 se publicó en el Diario Oficial la ley 21.096, que consagra la protección de datos personales como garantía constitucional, en el numeral 4° del artículo 19 de la Constitución.

[61] El artículo 12 de la Declaración señala: "Nadie será objeto de intromisiones arbitrarias en su vida privada, en la de su familia, o en su domicilio o correspondencia, ni de atentados a su honor y reputación. Toda persona tiene derecho a la protección de la ley contra tales intromisiones y atentados".

[62] En el artículo 17 del Pacto se establece: "Nadie será objeto de intromisiones ilegales o arbitrarias en su vida privada, su familia, su domicilio o correspondencia, ni de ataques ilegales a su honra o reputación. Toda persona tiene derecho a la protección de la ley contra esas injerencias o ataques".

[63] El artículo 8 del Convenio de Roma, dispone: "Toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de su correspondencia. No podrá haber injerencia de la autoridad pública en el ejercicio de este derecho si no en tanto esta injerencia este prevista por la ley y constituya una medida que, en una sociedad democrática, sea necesaria para la seguridad nacional, seguridad pública y el bienestar económico del país, la defensa del orden y la prevención del delito, la protección de la salud o de la moral, o la protección de los derechos y libertades de los demás".

[64] Rebollo Delgado, L. (2000), "*El derecho fundamental a la intimidad*", Madrid, Dykinson, pp. 60 y ss.

Brandeis, abogados norteamericanos que estudiaron Derecho en la *Harvard Law School*, y son considerados los padres del derecho a la intimidad[65]. En su trabajo plantean que el ciudadano tiene derecho a que la autoridad, la prensa o terceros se mantengan alejados de una esfera que solo le pertenece al individuo, así estatuyen las bases de la noción de *privacy*, configurándola como un derecho a la soledad, pasando a configurar la intimidad una doble perspectiva; por una parte la intimidad se configura en una dimensión conservadora o restrictiva, como instrumento para no proporcionar a las autoridades información o antecedentes personales, pecuniarios y patrimoniales con la finalidad de eludir la presión fiscal del Estado. Por otra parte, la dimensión progresista o extensiva configura la intimidad para contravenir el acopio de datos dirigidos al control de comportamientos ideológicos con fines discriminatorios.

Si bien Warren y Brandeis originalmente configuran el derecho a la intimidad en relación con el derecho de propiedad, paulatinamente van acercándolo al derecho de propiedad intelectual y luego a contenidos más inmateriales, dotando al derecho a la intimidad de mayor autonomía. En esta evolución, el presupuesto o antecedente del *privacy* estará en las libertades individuales, configurándose como un derecho completamente autónomo.

Un análisis interesante de las implicancias teóricas del concepto de *privacy* lo expone Michele Bocchiola en el capítulo quinto de su obra *"Privacy, Filosofía e Politica di un Concetto Inesistente"*, argumentando que existen cuatro maneras de aproximarse al mismo, las que Revenga Sánchez[66] resume de la siguiente manera: "La primera de ellas es la que se construye a partir de la celebérrima definición de Warren y Brandeis (…) insiste en el valor que tiene, de por sí, la posibilidad de disponer de un espacio/fortaleza en el que cada individuo pueda desempeñarse libre de intromisiones ajenas. La segunda, considera que el respeto por parte de los poderes públicos y por parte de los particulares de un ámbito de vida privada es una condición necesaria para poder tomar decisiones de manera autónoma e independiente; la *privacy* equivale aquí a autonomía decisoria. Y la tercera y cuarta de tales aproximaciones generales insisten en la centralidad de la información y del control sobre ellas en las sociedades de nuestros días; la tercera para atribuir al derecho en cuestión la cualidad de fundamentar limitaciones estrictas al acceso(…) a ciertas informaciones relacionadas con la vida personal de cada uno(…) y la cuarta y última, para insistir en que lo importante no es tanto limitar como

[65] La causa de la publicación de este artículo se encuentra en que la señora Warren y su marido, que constituían una familia acaudalada de Boston, regularmente celebraban fiestas que reunían a la alta sociedad de la época, llamando la atención y despertando el interés de la prensa local que informaba lo sucedido en aquellos encuentros, entregando datos personales y sensibles de los asistentes, induciendo al lector a imaginarse conductas anormales y disipadoras de la alta sociedad, llegando incluso a tergiversar lo ocurrido en la fiesta que Warren celebra en honor de la boda de su hija, lo que lo motiva a reunirse con Brandeis para configurar un nuevo derecho.

Tres años después, de la publicación del artículo de Warren y Brandeis, el Tribunal Supremo de Nueva York, en diciembre de 1893, en la causa Marks vs Jaffa, dictaminó que el demandante tenía "derecho a ser dejado en paz". *The courts will in such cases secure to the individual what has been aptly termed the right "to be let alone."* (En tales casos, los tribunales garantizarán al individuo lo que se ha denominado acertadamente el derecho a "que lo dejen solo"). El asunto se inicia cuando el periódico *Der* Wachter publicó un retrato del demandante, incluyéndolo sin su consentimiento y con su oposición, en una competición de popularidad con otro actor. Se invitaba a los lectores a votar por uno o por otro.

[66] Revenga Sánchez, M. (2014), "El Derecho a la Intimidad: un derecho en demolición (y necesitado de reconstrucción)" en *Cuadernos y Debates* n°248: El derecho a la privacidad en un nuevo entorno tecnológico. Madrid. Centros de Estudios Políticos y Constitucionales, pp. 71-98.

conocer (y disponer de la posibilidad de controlar y limitar) el uso que puede hacerse de la información que nos afecta y que se halla en manos de terceros."

Diversas han sido las corrientes doctrinarias que se han abocado a la conceptualización del derecho a la intimidad, así José Luis Concepción[67] sostiene que en la intimidad del hombre se desarrolla su humanidad y su personalidad, como consecuencia y como fruto de la libertad para la toma de decisiones y para elegir sus propias normas de conciencia, sus creencias y su ideología entre otros aspectos. Por su parte, Judith Thompson[68] plantea que "el derecho a la intimidad no es en realidad, un derecho independiente si no que deriva de otros, como el derecho de propiedad o el derecho a no ser observado". Luis García San Miguel[69] sostiene que "la intimidad es el derecho a que ciertos aspectos de nosotros mismos no sean conocidos por los demás, una especie de derecho al secreto, a que los demás no sepan lo que somos, lo que sentimos y lo que hacemos." A su turno Rebollo Delgado[70] señala que cuando el ordenamiento jurídico español se refiere a la intimidad, como analogía al término privacidad se ha referido tanto al derecho a la intimidad en sentido estricto, como al derecho al honor, como al derecho a la propia imagen.

Por otra parte, la Constitución de la República de Brasil, en el artículo quinto, inciso décimo, establece que son inviolables la intimidad, la vida privada, el honor y la imagen de las personas, asegurando el derecho a la indemnización de daño material o moral. Tal como se recoge en el capítulo primero "De los derechos individuales y colectivos", Título II, "De los derechos y garantías individuales". En ese contexto normativo la doctrina[71] ha delimitado la privacidad de la intimidad, señalando respecto de esta última que fija una división lineal entre el yo y los otros, de forma que crea un espacio que el titular desea mantener impenetrable incluso a los más cercanos, de manera tal que el derecho a la intimidad tiene importancia y significación jurídica en la protección del individuo exactamente para defenderlo de lesiones a derechos dentro de la interpersonalidad de la vida privada.

En la doctrina chilena, Nogueira[72] plantea que "La intimidad es el ámbito reservado del individuo que no desea ser develado al conocimiento y acción de los demás, el cual aparece como necesario para mantener un mínimo de calidad de vida humana. El derecho a la intimidad es la facultad de la persona para evitar las injerencias de terceros en el ámbito de su privacidad, salvo la autorización de tal develamiento de la intimidad por el propio afectado. La intimidad de la persona es una zona intrínsecamente lícita, que merece respeto y protección a nivel constitucional".

---

[67] Concepción Rodríguez, J. L. (1996), "Honor, intimidad e imagen: un análisis jurisprudencial de la L.O 1/1982", Barcelona, Boch.

[68] Thompson, J. en Nino C.S. (2002), "Fundamentos de Derecho Constitucional, análisis filosófico, jurídico y politológico de la práctica constitucional". Buenos Aires, Editorial Astrea, p.328.

[69] García San Miguel, L. (1992), "*Estudios sobre el derecho a la intimidad*", Alcalá de Henares, Madrid. Tecnos, p.17.

[70] Rebollo Delgado, L. (1998), "Derechos de la personalidad y datos personales", *Revista de Derecho Político*, n° 44, Madrid, p.167.

[71] Araujo, L. y Serrano, N., (2011), "*Curso de direito constitucional*", 15° ed. São Paulo, Editora Verbatim, p.183.

[72] Nogueira Alvalá, H. (1998), "El Derecho a la Privacidad y a la Intimidad en el Ordenamiento Jurídico Chileno" en *Ius et Praxis*, vol. 4, núm. 2, Universidad de Talca, Talca, Chile, pp. 65-106.

El derecho a la intimidad, que está comprendido en el derecho a la privacidad, tiene entonces un carácter más estricto y una dimensión individual que abarca como aspectos básicos la concepción religiosa e ideológica, la vida sexual, el estado de la salud, la intimidad corporal o pudor, entre otros. Así, precisando en el ámbito constitucional positivo chileno, como ya se señaló, el artículo 19, N°4, asegura cuatro dimensiones del derecho: a) el derecho al respeto y protección de la vida privada de las personas; b) el derecho al respeto de la vida pública de las personas; c) el derecho al respeto de la honra de la persona y de su familia; d) el derecho y protección de sus datos personales.

El respeto implica la obligación de terceras personas, sean naturales o jurídicas, públicas o privadas, en orden a no interferir en el ámbito del valor y conducta protegido jurídicamente, el cual recibe la protección del Estado a través del conjunto de garantías que brinda a tales bienes jurídicos y a sus titulares para defenderlos y exigir que ellos sean respetados.

Así entonces, el derecho a la intimidad es un derecho de la personalidad que tiene por objeto asegurar a la persona un ámbito reservado de su vida vinculado con el respeto a su dignidad como ser humano. El valor o bien jurídico protegido es el respeto a la existencia de un ámbito propio y reservado de la vida, frente a la actividad y conocimiento de los demás, sean estos autoridades o particulares.

El Derecho a la Privacidad y a la Vida Privada

Abordar la noción de vida privada o de privacidad no es tarea fácil, de eso indiscutiblemente dan cuenta no solo la doctrina y la jurisprudencia, sino también los ordenamientos jurídicos positivos, que ya sea constitucional o legalmente en muchos casos les dan un mismo tratamiento, a pesar de ser nociones distintas[73], o definitivamente no los conceptualizan.

El concepto de vida privada es un concepto variable en el tiempo, el ámbito de la vida privada es aquel donde el individuo actúa como parte de un pequeño grupo o de una pequeña unidad (familia, círculo de amigos), que reclama y está preparada, como dice Westin, para ejercer una segregación corporativa, permitiendo alcanzar relaciones francas, relajadas y cerradas entre dos o más personas[74].

Lo privado es un ámbito no público, que se excluye del conocimiento abierto, en el que se practican un determinado tipo de relaciones interpersonales, entre ellas debe incluirse cierto tipo de relaciones profesionales, como, por ejemplo, las que tiene el médico con su paciente o el abogado con su patrocinado, que están estrechamente vinculadas con la privacidad.

El concepto de vida privada no fue precisado por el constituyente chileno, es por consiguiente al igual que la intimidad, un concepto jurídico constitucional indeterminado, cuya delimitación

[73] "La idea de privacidad implica la posibilidad irrestricta de realizar acciones privadas, o sea acciones que no dañan a terceros y que, por lo tanto, no son objeto de calificación por parte de una moral pública como la que el derecho debe imponer, ellas son acciones que, en todo caso, infringen una moral personal privada que evalúa la calidad de carácter o de la vida de la agente y son, por lo tanto, acciones privadas, por más que se realicen a la luz del día y con amplio conocimiento público". Véase: Nino, C.S. (2002), "*Fundamentos de Derecho Constitucional, Análisis filosófico, jurídico y politológico de la práctica constitucional*", Buenos Aires, Editorial Astrea, p.327.

[74] Ver Westin, A. F., (1970), "*Privacy and Freedom*," Ed. Atheneum, 6ª edición, Nueva York, p. 31.

y configuración quedó entregada a la doctrina y jurisprudencia, sin perjuicio de las configuraciones que haga el legislador.

Sagüés[75]hace un esfuerzo por delimitar el ámbito privado del público para lo cual distingue dos tipos de actuaciones privadas, las internas y las externas.

Las acciones privadas internas se configuran por los comportamientos o conductas íntimas o inmanentes que principian y concluyen en el sujeto que las realiza, no trascendiendo de este, comprendiendo los hechos o actos realizados en absoluta privacidad o de los que nadie puede percatarse. Las acciones privadas externas son conductas o comportamientos que trascienden al sujeto que las realiza, siendo conocidas por los demás, pero que no afectan ni interesan al orden o la moral pública, ni causan perjuicios a terceros, vale decir, no afectan al bien común.

Ambas dimensiones conforman parte del derecho al respeto de la vida privada de las personas y su familia que el Estado debe asegurar, garantizar y promover, lo que las diferencia claramente de las acciones públicas. En efecto, las acciones públicas son acciones externas que trascienden a quien las ejecuta, ya que pueden afectar el orden o la moral pública o causar daños a terceros, por lo que el Estado puede regularlas y, eventualmente, prohibirlas.

Sin perjuicio de las reflexiones ya hechas en esta materia, resulta adecuada la conceptualización de vida privada que nos entrega Espín Templado, para el cual vida privada "es el conjunto de circunstancias y datos relativos a la vida de una persona que quedan fuera del conocimiento de los demás, salvo que medie un expreso deseo de comunicarlo o de ponerlo de manifiesto por parte de la persona afectada y al margen, naturalmente, de las personas que comparten con ellos aspectos más o menos amplios de su vida" [76].

De igual modo, los tribunales internacionales de derechos humanos han consensuado que la vida privada es un concepto amplio de mayor extensión que el del derecho a la privacidad y que por lo tanto lo incluye. Entonces para los efectos de este trabajo nos centraremos mayoritariamente en el derecho a la vida privada, en el entendido que la privacidad es parte de esta, constituyendo ambos (vida privada y privacidad), antecedentes del derecho a la protección de datos personales[77].

A diferencia del derecho a la intimidad, el derecho a la vida privada sí se ha consagrado expresamente en diferentes instrumentos jurídicos, sean declaraciones, convenios o pactos internacionales tanto a nivel global como regional (europeo y americano). Desde la perspectiva global se refieren a este el artículo 12 de la Declaración de los Derecho Humanos, así también el artículo 17 del Pacto de Derechos Civiles y Políticos de 1966, el artículo 14 de la Convención Internacional sobre la protección de los derechos de todos los trabajadores migratorios y de

[75] Sagüés, N. (1997), "*Elementos de Derecho Constitucional*", tomo 2, 2da. edición actualizada, Ed. Astrea, Buenos Aires, Argentina, p.314.

[76] Espín Templado, E. (1991), "Fundamento y alcance del derecho fundamental a la inviolabilidad del domicilio", *Revista del Centro de Estudios Constitucionales*, nº 8, Madrid, España, p.45.

[77] En la práctica existen referencias a la privacidad y a la vida privada como un mismo derecho en varios instrumentos internacionales. Sobre el particular véase la Resolución 68/167, de 21 de enero de 2014, el derecho a la privacidad en la era digital, aprobada por la Asamblea General de la Organización de Naciones Unidas (ONU) el 18 de diciembre de 2013, misma que se refiere al "derecho humano a la privacidad" pero utiliza también le término vida privada, consagrado en los artículos 12 de la Convención Universal de Derechos Humanos y 17 del Pacto Internacional de Derechos Civiles y Políticos.

sus familiares de 1990, como también lo hace en su artículo 16 la Convención de los Derechos del Niño de 1989. En el ámbito regional, a nivel americano, el derecho a la vida privada está reconocido expresamente en el artículo 11.2 de la Convención Americana de Derechos Humanos o Pacto de San José: "Nadie puede ser objeto de injerencias arbitrarias o abusivas en su vida privada, en la de su familia, en su domicilio o en su correspondencia, ni de ataques ilegales a su honra o reputación". En el ámbito europeo el artículo 8.1del Convenio para la Protección de los Derechos y Libertades Fundamentales o Convención Europea de Derechos Humanos: "Toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de su correspondencia".

De igual forma y coincidente con su consagración expresa en diversos instrumentos internacionales, en la jurisprudencia internacional el derecho a la vida privada ha tenido un abundante tratamiento y ha permitido ir perfilando, como veremos, el derecho a la protección de datos como un derecho autónomo e independiente. A continuación, a modo referencial, nos centraremos en algunos de los criterios del Tribunal Europeo de Derechos Humanos y de la Corte Interamericana de Derechos Humanos que así lo demuestran.

Jurisprudencia del Tribunal Europeo de Derechos Humanos (TEDH) sobre la vida privada

Tal como lo plantean Maqueo, Moreno y Recio[78], el Tribunal Europeo de Derechos Humanos (TEDH) en relación con el artículo 8 del Convenio Europeo de Derechos Humanos aborda posibles limitaciones en la vida privada y familiar de las personas. La primera sentencia del TEDH sobre la vigilancia secreta de los Estados, por medio de la efectiva interceptación de comunicaciones por necesidades de orden criminal o de seguridad nacional se encuentra en el caso Klass (TEDH 1978\1)[79]. Sustentado en esa sentencia que considera que no se ha violado el artículo 8 del Convenio Europeo para la protección de los Derechos Humanos y las Libertades Fundamentales, el Tribunal empieza a interpretar la admisibilidad de las restricciones a la vida privada. Aunque el TEDH admite que los Estados firmantes de la Convención tienen cierta discreción respeto de los términos en los que operan sus sistemas de vigilancia de las comunicaciones, no se trata de una discrecionalidad absoluta. Para que esta limitación sea admisible deben darse las siguientes circunstancias: i) que persiga un objetivo legítimo y lo es la seguridad nacional y/o la defensa del orden y la prevención de los delitos; ii) que esté prevista en una ley; y iii) que sea necesaria en una sociedad democrática.

Lo anterior implica entonces adoptar garantías adecuadas y efectivas contra los eventuales abusos que pudiera ocasionar la autoridad[80].

Sobre los supuestos o requisitos señalados, el Tribunal ha establecido criterios que es posible sistematizar de la siguiente manera: en lo que dice relación con la persecución de un fin

---

[78] Maqueo Ramírez, M., Moreno González, J. y Recio Gayo, M. (2017), "Protección de datos personales, privacidad y vida privada: la inquietante búsqueda de un equilibrio global necesario", en *Revista de Derecho*, Vol. XXX, n°1, junio, Valdivia, pp. 77-96.

[79] TEDH, Klass and others v. Germany, Sentencia de 6 de septiembre de 1978, parr. 39 y ss.

[80] THDE, Malone v. The United Kingdom, Sentencia de 2 de agosto de 1984, párr. 63 y ss. y TEDH, Kruslin v. France, Sentencia de 24 de abril de 1990, párr. 27 y ss., entre otros.

legítimo, el Tribunal ha analizado varios casos en los que se considera que se cumple este requisito, por ejemplo, en la adopción de medidas para garantizar la seguridad nacional y la prevención del desorden o el delito e, incluso, posteriormente, en relación con la transferencia de datos de salud de una autoridad a otra para decidir respecto de la asignación de recursos públicos[81].

En relación con que la interferencia o afectación este prevista en la ley, el TEDH dispone que además de encontrar sustento en la legislación nacional, es necesario considerar la calidad de la ley y su *foreseeability*, esto es, que contribuya a fortalecer el Estado de derecho. Así, el Tribunal establece que el requerimiento de que la medida sea *"de acuerdo con la ley"* supone que existe una previsión legal previa y que la ley sea accesible y suficientemente clara respecto de las circunstancias y condiciones en las que las autoridades están facultades para establecer estas interferencias, estableciendo a su vez medidas adecuadas de protección legal.

Por último, el requerimiento de que las interferencias sean necesarias en una sociedad democrática implica la identificación, dentro del ámbito más amplio del objetivo legítimo perseguido, de la necesidad social específica que deba abordarse, la proporcionalidad de la medida para alcanzar dicho objetivo legítimo y que existan razones relevantes y suficientes que la justifiquen debido a otras posibles medidas.[82]

Determinante para que el Tribunal Europeo se pronunciara sobre campos propios del derecho a la protección de datos personales, en un principio referidos al acceso a la propia información personal registrada en archivos públicos, fue el reconocimiento de que si bien el artículo 8 del Convenio Europeo tiene, como se ha señalado, fundamentalmente por objeto proteger a los individuos en contra de interferencias arbitrarias por las autoridades públicas, también podría incluir obligaciones positivas del Estado, inherentes al respeto efectivo de la vida privada y familiar, de tal forma que incluso la negativa para conceder acceso a la información personal del individuo debe analizarse "por una autoridad independiente", bajo la perspectiva de los supuestos que establece el artículo 8 antes indicado, con el fin de garantizar la aplicación del principio de proporcionalidad[83].

Así, el Tribunal reconoce que el artículo 8 protege, entre otros intereses, el derecho al desarrollo personal, lo que incluye el derecho de recibir información relativa a su identidad personal, necesaria para conocer sus orígenes y entender su infancia y posterior desarrollo[84].

Las primeras referencias explicitas que el TEDH realiza a la protección de datos personales se relacionan con datos de salud, que contienen información sensible[85]. El Tribunal analiza si las medidas que se impugnan, relacionadas con obtener y mantener la confidencialidad de

---

[81] TEDH, M. S. v. Sweden, Sentencia de 2 de agosto de 1997, párr. 32 y ss; y TEDH, Leander v. Sweden, Sentencia de 26 de marzo de 1987, párr. 48 y ss.

[82] Grupo de Trabajo del Artículo 29 sobre la Protección de Datos, Dictamen 1/2014 sobre la aplicación de los conceptos de necesidad, proporcionalidad y la protección de datos en el sector de los organismos con funciones coercitivas, adoptado el 27 de febrero de 2014, p.6 y ss.

[83] TEDH, Gaskin v. The United Kingdom, Sentencia de 7 de julio de 1989, párr. 49:.

[84] TEDH, Odièvre v. France, Sentencia de 13 de febrero de 2003, párr. 25 y ss. y X and Y v. Netherlands, Sentencia de 26 de marzo de 1985, párr. 28 y ss.

[85] TEDH, Z. v. Finland, Sentencia del 25 de febrero de 1997, párr. 72 y ss.; TEDH, M. S. v. Sweden, Sentencia de 2 de agosto de 1997, párr. 32 y ss.

información médica de una pareja con VIH, información que también consta en otro expediente de un juicio seguido contra uno de los integrantes de dicha pareja, relativo a delitos de índole sexual. Cuestionándose el órgano jurisdiccional internacional si estas medidas son necesarias o se justifican en una sociedad democrática.

Sobre el punto, el TEDH sostiene que la confidencialidad de los datos de salud es un principio vital de los ordenamientos jurídicos de los Estados que integran el Convenio. Resulta clave no solo desde la perspectiva de respetar la privacidad de los pacientes sino también para mantener la confianza en los servicios de salud y en la profesión médica.

De igual forma el Tribunal dispone que todas estas consideraciones se vuelven aún más sensibles cuando se trata de la confidencialidad de información relacionada con una persona infectada de VIH, por cuanto la develación de esta información puede afectarla dramáticamente en su vida privada y familiar, como también laboral y social, exponiéndola al oprobio y ostracismo[86].

Posteriormente, el TEDH reconoce explícitamente que la transferencia de datos de salud de una autoridad a otra, sin el consentimiento del paciente y que, a su vez, ha servido para diferentes propósitos, constituye una interferencia en el derecho al respeto de la vida privada y familiar del paciente. En ese sentido, el Tribunal establece que las medidas adoptadas para la comunicación de la información entre autoridades se deben analizar a la luz de los supuestos o requerimientos previamente establecidos[87].

De igual forma, bajo la idea de que el término "*vida privada"* no debe ser interpretado de manera restrictiva, la Corte incluye dentro del ámbito de protección del tantas veces referido artículo 8, el almacenamiento de datos relativos a una persona, con independencia de si los mismos son o no sensibles, lo que, de acuerdo con el propio Tribunal, es consistente con el Convenio 108 del Consejo de Europa[88]. Estas consideraciones se hacen extensivas también al uso de la información, lo que incluye su divulgación por parte de las autoridades, y a la falta de medios para refutar el contenido de dicha información[89].

Sucesivamente, el Tribunal reitera las obligaciones positivas del Estado para proteger la vida privada de las personas que se derivan del punto 1 del artículo 8 del Convenio Europeo, lo que lo lleva a considerar la posibilidad de que, incluso, la divulgación de información por parte de personas distintas a las autoridades, incluida la prensa y los medios de comunicación masiva, sea contraria a los términos de la Convención[90].

Del mismo modo y consistente con las obligaciones positivas que conlleva el citado artículo 8 del Convenio, el Tribunal reitera el deber de proporcionar a las personas "un procedimiento

---

[86] TEDH, Z. v. Finland, cit., párrs. 111 y 112. Sobre el particular también véase TEDH, I. v. Finland, Sentencia de 17 de octubre de 2008, párr. 35.

[87] TEDH, M.S. v. Sweden, cit., párr. 32 y ss.

[88] TEDH, Amann v. Switzerland, Sentencia de 16 de febrero de 2000, párr. 65.

[89] TEDH, Rotaru v. Romania, Sentencia del 4 de mayo de 2000, párr. 46 y TEDH, Peck v. United Kingdom, Sentencia de 28 de enero de 2003, párr. 57 y ss.

[90]TEDH, Von Hannover v. Germany (No. 2), Sentencia de 7 de febrero de 2012, párr. 74 y ss.; y Sciacca v. Italy, Sentencia de 11 de enero de 2005, párr. 27 y ss.

efectivo y accesible" para obtener el acceso a "información relevante y apropiada" de los archivos personales mantenidos por las autoridades[91].

Como se puede observar, el TEDH va perfilando la inclusión del derecho a la protección de datos personales en relación con el derecho a la vida privada. Incluso, ya establece en sus decisiones esta conexión al indicar textualmente que "La protección de datos de carácter personal juega un rol fundamental en el ejercicio del derecho al respeto de la vida privada y familiar consagrado en el artículo 8 de la Convención". Acerca del particular se señala que el mero hecho de que la legislación interna facilite la oportunidad de reclamar indemnizaciones por daños y perjuicios por la revelación ilegal de los datos personales no es razón suficiente para proteger la vida privada, es necesario que los Estados firmantes de la Convención provean de una protección "real y efectiva" que excluya cualquier posibilidad de acceso no autorizado[92]. Lo anterior es consistente con la idea central de que el derecho a la vida privada "es un término amplio no susceptible de una definición exhaustiva, que comprende la integridad física y psicológica de una persona y puede comprender múltiples aspectos de la identidad de la persona"[93].

Al igual que lo que ocurre con el término "vida privada", la expresión "dato personal" es una expresión amplia, siendo omnicomprensiva, según el TEDH, de muy diversos ámbitos de la información de una persona identificada o identificable, los que van desde el propio nombre, la fecha de nacimiento y el historial médico, hasta las huellas dactilares, muestras de células y elaboración de sus perfiles de ADN, entre otros[94].

Jurisprudencia de la Corte Interamericana de Derechos Humanos (CIDH) sobre la vida privada

Tradicionalmente la Corte ha establecido que el derecho a la vida privada implica una obligación negativa para el Estado, así en una primera etapa, lo ha relacionado con la inviolabilidad del domicilio, de tal forma que la intromisión en el domicilio familiar de las personas, sin el consentimiento de quienes lo habitan y sin autorización legal para ello, así como su propia destrucción, se consideran una violación grave, injustificada y abusiva a los términos del artículo 11.2 de la Convención Americana de Derechos Humanos[95].

Asimismo, la Corte considera que "…el ámbito de la privacidad se caracteriza por quedar exento e inmune a invasiones agresivas o arbitrarias por parte de terceros o de la autoridad pública". Además, establece que las injerencias en la vida privada de las personas deben: (1)

---

[91]TEDH, Haralambie v. Romania, Sentencia de 27 de octubre de 2009, párr. 86.

[92] TEDH, B.B. v. France, Sentencia de 17 de diciembre de 2006, párr. 61.

[93] TEDH, Axel Springer AG v. Germany, Sentencia de 7 de febrero de 2012, párr. 83.

[94] TEDH, S. and Marper v. United Kingdom, Sentencia de 4 de diciembre de 2008, párr. 71; K.U. v. Finland, Sentencia de 2 de diciembre de 2008, párr. 41 y ss.; Khelili v. France, 18 de octubre de 2011, párr. 56; y, M.K. v. France, Sentencia de 18 de abril de 2013, párr. 29.

[95] CIDH, Caso Masacres de Ituango vs. Colombia, Sentencia de Fondo, de 1 de julio de 2006, párr. 197; CIDH, Caso Escué Zapata vs. Colombia, Sentencia de Fondo (Reparaciones y Costas), de 4 de julio de 2007, párrs. 94 y 96. Más adelante, la CIDH retoma este criterio en el Caso Familia Barrios vs. Venezuela, Sentencia de Fondo (Reparaciones y Costas), de 24 de noviembre de 2011, párr. 140.

estar previstas en la ley, (2) perseguir un fin legítimo, y (3) ser idóneas, necesarias y proporcionales.

Es decir, los requisitos que han de cumplir los límites al derecho a la vida privada comprenden tanto el principio de proporcionalidad en términos de Alexy (compuesto por sus tres subprincipios: idoneidad, necesidad y proporcionalidad en sentido estricto)[96], como el principio de legalidad. En caso de no cumplir con estos requisitos, las injerencias se consideran contrarias a los términos de la propia Convención[97].

La Corte dispone que, a pesar de no señalarse explícitamente en el texto de la Convención, la vida privada tiene alcances más allá del domicilio y la correspondencia, incorporando otros aspectos como la intervención, monitoreo, grabación y divulgación de conversaciones por vía telefónica[98]. En ese sentido se reconoce que "la fluidez informativa que existe hoy coloca al derecho a la vida privada de las personas en una situación de mayor riesgo debido a las nuevas herramientas tecnológicas y su utilización cada vez más frecuente". De ahí que el Estado deba "asumir un compromiso aún mayor, con el fin de adecuar a los tiempos actuales las formas tradicionales de protección del derecho a la vida privada".

Así, la Corte de manera consistente con sus resoluciones previas, manifiesta que "el concepto de vida privada es un término amplio no susceptible de definiciones exhaustivas". Sin embargo, este concepto comprende, entre otras cosas, "la vida sexual y el derecho a establecer y desarrollar relaciones con otros seres humanos". De tal forma que las violaciones sexuales vulneran la vida privada de las personas, toda vez que impiden "el control sobre sus decisiones más personales e íntimas y sobre las funciones corporales básicas"[99]. En una concepción expansiva del derecho a la vida privada y su estrecha relación con otros derechos humanos reconocidos por la Convención Americana, la Corte señala que "la vida privada incluye la forma en que el individuo se ve a sí mismo y cómo y cuándo decide proyectarse a los demás".

La Corte retoma también los requisitos necesarios para considerar que una injerencia en la vida privada de las personas no se considere abusiva o arbitraria, volviendo a señalar que tanto la idoneidad, la necesidad, como la proporcionalidad de las medidas adoptadas implican que sean "necesarias en una sociedad democrática"[100].

Finalmente, en una resolución histórica relativa a la prohibición general de la fecundación in vitro concebida como una injerencia en la vida privada de las personas, la CIDH adopta de manera expresa criterios provenientes del Tribunal Europeo de Derechos Humanos, en el sentido de que el ámbito de protección del derecho a la vida privada va más allá del derecho a

---

[96] Cfr. Alexy, R., "Constitutional Rights and Proportionality," Revus, *Journal for constitutional theory and philosophy of law*, Nª. 22, 2014, p.52.

[97] CIDH, Caso Tristán Donoso vs. Panamá, Sentencia de Fondo (Excepción Preliminar, Fondo, Reparaciones y Costas), de 27 de enero de 2009, párrs. 55 y 76.

[98] Idem. y CIDH, Caso Escher y Otros vs. Brasil, Sentencia de Fondo (Excepción Preliminar, Fondo, Reparaciones y Costas), de 6 de julio de 2009, párr. 114.

[99] CIDH, Caso Fernández Ortega vs. México, Sentencia de Fondo (Excepción Preliminar, Fondo, Reparaciones y Costas), de 30 de agosto de 2010, párr. 129 y Caso Rosendo Cantú y Otra vs. México, Sentencia de Fondo (Excepciones Preliminares, Fondo, Reparaciones y Costas), de 31 de agosto de 2010, párr. 119.

[100] CIDH. Caso Atala Riffo y Niñas vs. Chile, Sentencia de Fondo (Reparaciones y Costas), de 24 de febrero de 2012, párr. 162.

la privacidad. De manera textual, la Corte ahonda en el concepto de vida privada, tomando criterios cuyo desarrollo corresponde al ámbito europeo:

"La protección a la vida privada abarca una serie de factores relacionados con la dignidad del individuo, incluyendo por ejemplo la capacidad para desarrollar la propia personalidad y aspiraciones, determinar su propia identidad y definir sus propias relaciones personales. El concepto de vida privada engloba aspectos de la identidad física y social, incluyendo el derecho a la autonomía personal, desarrollo personal y el derecho a establecer y desarrollar relaciones con otros seres humanos y con el mundo exterior. La efectividad del ejercicio del derecho a la vida privada es decisiva para la posibilidad de ejercer la autonomía personal sobre el futuro curso de eventos relevantes para la calidad de vida de la persona. La vida privada incluye la forma en que el individuo se ve a sí mismo y cómo decide proyectarse hacia los demás, y es una condición indispensable para el libre desarrollo de la personalidad"[101]

De lo expuesto, parece razonable señalar que ésta sentencia de la CIDH, que considera los criterios emitidos por su homóloga europea en materia del derecho a la vida privada, anticipan un desarrollo armónico de este derecho en ambos sistemas internacionales de derechos humanos.

Sin embargo, mientras el TEDH ha dado pasos significativos que permiten profundizar acerca de la noción misma del derecho a la protección de datos personales en su relación con el derecho a la vida privada, reconociendo que bajo el concepto de vida privada puede quedar amparada "toda información relativa a una persona física identificada o identificable", con independencia de si se trata o no de información sensible que afecta la esfera más íntima de las personas, lo que a su vez es consistente con la amplia definición de "dato personal". Como contrapartida la CIDH hasta la fecha aún no emite pronunciamiento alguno sobre el derecho a la protección de datos, pese a que varios países sometidos a su jurisdicción lo contemplan como un derecho ya sea en sus constituciones, leyes u ordenamientos jurídicos internos.

Relación entre la Intimidad, la Vida Privada y el Derecho a la Protección de Datos

Los derechos personalísimos permiten estructurar un espacio de libre configuración y desarrollo de la personalidad, lo que evidentemente supone una potestad de disposición o de control sobre estas facultades. Así lo plantea a propósito de la libertad de información Frosini, [102]cuando señala: "La libertad informativa representa una nueva forma de desarrollo de la libertad personal; no consiste únicamente en la libertad negativa del rigth of privacy (…) si no que consiste también en la libertad de informarse, es decir, de ejercer un control autónomo sobre los datos propios, sobre la propia identidad informática".

Resulta indudable que, con el desarrollo digital, el surgimiento de las redes sociales y la capacidad de interconexión y diálogo virtual que somos capaces de generar, las necesidades

[101] CIDH, Caso Artavia Murillo y Otros ("Fecundación in vitro") vs. Costa Rica, Sentencia de Fondo (Excepciones Preliminares, Fondo, Reparaciones y Costas), de 28 de noviembre de 2012, párr. 143.

[102] Frosini, V. (1988), "*Informática y Derecho*", trad. del italiano por Jorge Guerrero y Mariano Ayerra Redin, Bogotá., Temos, p. 23.

humanas empujen a una reformulación y actualización del contenido y alcances de los derechos.

En este mismo sentido, en la actual era digital es evidente que la libertad se ve afectada por técnicas informáticas, sean de control individual o colectivo, que interfieren con su ejercicio, en especial aquellas que se relacionan con el tratamiento de datos de carácter personal[103].

En efecto, debido a la revolución tecnológica y digital, vivimos en un mundo acompañado de una constante creación, almacenamiento e intercambio masivo de datos, en muchas ocasiones de carácter personal, que construyen identidades digitales y un cuerpo "electrónico", inseparable del cuerpo físico de la persona[104].

En este contexto y como se revisó en las líneas precedentes, el derecho a la protección de datos se nutre y relaciona con la intimidad, la privacidad y la vida privada, hasta el punto que en sus inicios el derecho a la protección de datos no tenía un nombre comúnmente aceptado pues se le denominaba de diferentes formas: intimidad informática[105], habeas data, derecho a la autodeterminación informativa, derecho a la autodeterminación informática o libertad informática entre otros.

Los fundamentos de este derecho que finalmente se va a denominar derecho a la protección de datos personales, tal como lo señala Rebollo[106], se encuentran en la dignidad de la persona enmarcada en un ámbito de libertad individual.

---

[103] Los datos de carácter personal, están definidos en el apartado 1 del artículo 4 del Reglamento General de Protección de Datos n° 2016/679: "como toda información de una persona física identificada o identificable ("el interesado"); se considera persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona."

[104] Rodotà, S. (2014), "*El derecho a tener derechos*", Bolonia, Trotta, Traducción de Revuelta López, J. M., p.151.

[105] Sobre como denominar el nuevo derecho, el profesor Manuel Sánchez de Diego Fernández de la Riva ya planteaba en 1992 que "Se han empleado los términos «derecho a la autodeterminación informativa» (Lucas Murillo, P. "*El derecho a la autodeterminación informativa*". Madrid (1992) como traducción de *Recht auf informationelle Selbstbestimmung* o también «derecho a la autodeterminación informática» para referirse a la protección del individuo contra la recogida, el almacenamiento, la utilización, la transmisión y, en su caso, la difusión de datos concernientes a una persona por medios automatizados. Sin embargo, la expresión «derecho a la autodeterminación» tiene en la actualidad, tanto en el derecho internacional como constitucional, y a nivel general, una significación muy precisa, referida a la capacidad de los pueblos a determinar su destino político-totalmente diferente a la que se le quiete dar.

Es por todo ello que proponemos el término derecho a la intimidad informática. Cierto que esta expresión no facilita la diferenciación con el derecho a la intimidad (esta es la razón que utiliza Lucas Murillo para optar por «derecho a la autodeterminación informativa», y que ello puede suponer un problema a la hora de configurar como autónomo este derecho). Sin embargo, una vez establecida la independencia del derecho a la intimidad informática respecto del derecho a la intimidad, la expresión «derecho a la intimidad informática» creemos que es la más adecuada, porque expresa el origen de este derecho y no induce a confusión con otros derechos totalmente distintos". Ver "La transparencia de las bases de datos como mecanismo de protección de la intimidad de las personas", en III Congreso Iberoamericano de Informática y Derecho, *Revista Informática y Derecho 4*, Actas (volumen I), Editorial Aranzadi, p.146.

[106] Rebollo Delgado, L. y Serrano Pérez, M. M. (2008), "*Introducción a la protección de datos*", Madrid, Dykinson, pp. 40 y 101.

A pesar de los evidentes vínculos que el derecho a la protección de datos tiene con el derecho a la intimidad, con la noción de privacidad y con el derecho a la vida privada, se trata de derechos autónomos con reglas jurídicas diferentes. En efecto, como señala Balducci[107], pese a ser la intimidad o la vida privada fundamento concreto de su protección o tutela, además de otros vínculos que comparten, son derechos distintos y autónomos; al igual como ocurre con otros derechos, como el secreto de las comunicaciones, el honor o el derecho a la propia imagen.

También Conde[108] se refiere a la relación y diferenciación entre la intimidad y la privacidad al señalar; "el ámbito de la intimidad forma parte de la privacidad y no al contrario. Aunque ambas son reservadas, la privacidad es preservada de quienes no forman parte de nuestro entorno personal".

En este mismo sentido Rebollo[109] sostiene que: "esta singularización del derecho a la protección de datos obedece a una pretensión clara, una mayor protección del individuo. A esta circunstancia hay que añadir (…) la respuesta del derecho a las posibilidades técnicas. Si como hemos visto aquellos prácticamente en cincuenta años han tenido una evolución vertiginosa, el derecho no ha tenido otro remedio que adecuarse a esta celeridad. Por ello, el derecho a la intimidad ha permanecido estable, sin modificaciones conceptuales, normativas o jurisprudenciales, significativas. Por el contrario, el derecho a la protección de datos es una de las áreas del derecho, y de forma concreta de los derechos fundamentales, que más ha evolucionado, mejor normado y con más medios de garantía y protección, tanto a nivel estatal como europeo"[110].

En el ámbito jurisprudencial, el Tribunal Constitucional español también diferencia la intimidad de la protección de datos personales, y lo hace de manera precisa en la STC 292/2000, al exponer sus diferencias en cuanto a su función, objeto y contenido[111]. En materia de función, mientras que la intimidad protege frente a invasiones al "ámbito de la vida personal y familiar que la persona desea excluir del conocimiento ajeno y de las intromisiones de terceros en contra de su voluntad", la protección de datos personales tiene por función garantizar a su titular "un poder de control sobre sus datos personales, sobre su uso y destino, con el propósito de impedir su tráfico ilícito y lesivo para la dignidad y derecho del afectado". Por ello, el objetivo del derecho a la protección de datos personales es más amplio que el de la intimidad, a este respecto el TC español dispone que "el objeto de protección del derecho fundamental a la protección de datos no se reduce solo a los datos íntimos de la persona, sino

---

[107] Balducci Romano, F. (2013), "*The Right to the Protection of Personal Data: a New Fundamental Rigth of the European Union"*, p.7, disponible en: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2330307. Consulta realizada el 10 de abril 2020.

[108] Conde Ortiz, C. (2005), "La Protección de datos personales. Un derecho autónomo con base en los conceptos de intimidad y privacidad", Madrid, Dykinson, p.99.

[109] Rebollo Delgado, L. y Serrano Pérez, M. M. (2008), "*Introducción a la protección de datos*", Madrid, Dykinson, p.102.

[110] Evidentemente como veremos en el desarrollo de este trabajo, esto no es así en el caso chileno, donde la Ley n° 19.628, que regula la protección de datos personales, no tiene un adecuado marco regulatorio, siendo el Habeas data allí establecido de difícil tramitación judicial, sumado a la ausencia de una entidad de control en la materia.

[111] STCE 292/2000 Fundamentos Jurídicos 5, 6 y 7.

que a cualquier tipo de dato personal, sea o no íntimo, cuyo conocimiento o empleo por terceros pueda afectar a sus derechos, sean o no fundamentales, porque su objeto no es solo la intimidad individual… si no los datos de carácter personal".

Precisamente, para un mejor tutelar de las personas, el marco regulatorio de estos derechos es diverso y de ello dan cuenta, como ya se señaló en líneas anteriores, diversos instrumentos jurídicos internacionales, concretamente la Carta de los Derechos Fundamentales de la Unión Europea (CDFUE)[112] que en sus numerales 7 y 8 regula el derecho a la vida privada y familiar y el derecho a la protección de datos de carácter personal respectivamente. Y es precisamente esta distinción, expresión de autonomía e independencia de ambos derechos.

Si bien el señalado artículo 8 no define qué se entiende por derecho a la protección de datos, sí establece que toda persona goza de esa tutela.

Resulta interesante respecto de ambos derechos (vida privada y familiar por un lado y protección de datos personales, por el otro), la explicación que desde la propia web consultada se hace de ambos preceptos[113]. En efecto, los derechos garantizados en el artículo 7 de la Carta corresponden a los que garantiza el artículo 8 correspondiente del Convenio Europeo de Derechos Humanos (CEDH). A fin de tener en cuenta la evolución técnica, se ha sustituido la palabra "correspondencia" por "comunicaciones".

De conformidad con lo dispuesto en el apartado 3 del artículo 52, este derecho tiene el mismo sentido y alcance que en el CEDH. Como consecuencia de ello, las limitaciones de que puede ser objeto legítimamente son las mismas que las toleradas en el marco del referido artículo 8:

"1. Toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de su correspondencia.

2. No podrá haber injerencia de la autoridad pública en el ejercicio de este derecho, sino en tanto en cuanto esta injerencia esté prevista por la ley y constituya una medida que, en una sociedad democrática, sea necesaria para la seguridad nacional, la seguridad pública, el bienestar económico del país, la defensa del orden y la prevención del delito, la protección de la salud o de la moral, o la protección de los derechos y las libertades de los demás."

A su turno, la explicación sobre el derecho a la protección de datos de carácter personal establecido en el artículo 8 de la Carta, dispone que "este artículo se ha basado en el artículo 286 del Tratado constitutivo de la Comunidad Europea y en la Directiva 95/46/CE del Parlamento Europeo y del Consejo, relativa a la protección de las personas físicas en lo que

[112] Parece importante precisar que el derecho de protección de datos en la señalada Carta se establece en el Título relacionado con las libertades, derechos y principios derivados de las tradiciones y obligaciones constitucionales comunes de los Estados. Así se le reconoce a este derecho con el máximo rango posible de un derecho fundamental al interior de la Unión Europea, al constitucionalizarse a través de su incorporación al texto, y este a su vez elevarse con el mismo valor que los tratados fundacionales.

[113] http://www.derechoshumanos.net/normativa/normas/europa/CDFUE/CartaDerechosFundamentalesUnionEuropea-v2007.htm Consulta realizada el 10.04.2020.

respecta al tratamiento de datos personales y a la libre circulación de estos datos (DO L 281 de 23.11.1995, p. 31), así como en el artículo 8 del CEDH y en el Convenio del Consejo de Europa para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, de 28 de enero de 1981, ratificado por todos los Estados miembros. El artículo 286 del Tratado CE ha sido sustituido por el artículo 16 del Tratado de Funcionamiento de la Unión Europea y el artículo 39 del Tratado de la Unión Europea. Conviene señalar asimismo el Reglamento (CE) n° 45/2001 del Parlamento Europeo y del Consejo, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones y los organismos comunitarios y a la libre circulación de estos datos (DO L 8 de 12.1.2001, p. 1). La Directiva y el Reglamento mencionados establecen condiciones y límites para el ejercicio del derecho a la protección de los datos de carácter personal".

Así, el derecho a la vida privada y familiar contiene una tutela de carácter negativo, esto es, la obligación de no realizar intromisiones e interferencias ajenas. En cambio, el derecho a la protección de datos contiene una tutela de carácter positiva, al establecer la autodeterminación de cada individuo respecto de los datos de carácter personal.

Concordante con ello, Rodatà señala que: "la distinción (del articulado en la Carta de Derechos Fundamentales de la Unión Europea (CDFUE) no es solo de fachada. En el derecho del respeto a la vida privada y familiar se expresa ante todo un momento individual, el poder se agota en la exclusión de interferencias ajenas: la tutela es estática, negativa. La protección de datos, sin embargo, fija reglas ineludibles sobre las modalidades de su tratamiento y se concretizan en poderes de intervención"[114].

En este mismo sentido el concepto de intimidad o *privacy*, en el que según algunos autores se encontraría comprendida la protección de datos personales, "exige una respuesta acorde a una sociedad avanzada en la que la intimidad no tiene solo una faceta negativa o de abstención de injerencia en los poderes públicos. La protección de datos ha sido objeto de trato específico en la Carta de Niza, superando incluso al propio derecho al respeto a la vida privada y familiar que se consagra en el Convenio de Roma, para contemplar una dimensión activa que se traduce en todo un haz de facultades que permitirían al sujeto titular del derecho ejercer el control y gobierno de sus propios datos personales, así como defenderlos ante autoridades independientes".[115]

La noción de autocontrol sobre los datos personales permite entender de mejor forma que un dato personal pueda divulgarse públicamente siempre que su tratamiento se ajuste a los estándares o presupuestos determinados por el contenido mismo del derecho a la protección de datos. Así, por ejemplo, el nombre, la dirección o teléfono de una persona, contenido en una

[114] Rodotà, S. (2014), "*El derecho a tener derechos*", Bolonia, Trotta, Traducción de Revuelta López, J. M., pp.360-361.

[115] Tur Austina, R. (2006), "Cooperación en materia de terrorismo, transferencia de datos personales". Comentario a la sentencia del Tribunal de Justicia de la Unión Europea de 30 de mayo de 2006. *Revista Europea de Derechos Fundamentales*, n°8 (2) p.229.

guía telefónica, pueden darse a conocer sin la necesidad del consentimiento de su titular[116]. Ahora bien, si para el tratamiento de ese dato debe respetarse el principio de finalidad, es una cuestión irrelevante para el respeto y protección a la vida privada, pero trascendental para el derecho a la protección de datos de carácter personal y su adecuada tutela. De igual forma, como señala Contreras[117], las facultades que el derecho entrega a su titular, con independencia de la licitud del tratamiento que un tercero haga respecto de los datos personales en cuestión. En términos sencillos, una empresa puede haber celebrado un contrato con un individuo y en virtud de ello efectuar el tratamiento de datos personales. Pero el titular siempre podrá revocar el consentimiento o ejercer el derecho de oposición o cancelación sobre los datos personales que esa empresa está tratando. Esta dimensión del derecho a la protección de datos no tiene punto de relación con el derecho al respeto y protección de la vida privada.

La regulación normativa del derecho a la protección de datos personales tiene y tendrá diversas implicancias jurídicas, especialmente no solo en su relación, como ya hemos visto, con el derecho a la intimidad, a la privacidad, o a la vida privada, sino también con otros derechos con los que se relaciona e interactúa, como el derecho al acceso a la información pública, la libertad de expresión o el derecho al olvido.

En el caso chileno, esto será especialmente significativo, por su reciente reconocimiento constitucional en el N° 4 del artículo 19, que lo sitúa como una garantía constitucional explícita que además permite una acción constitucional efectiva, el recurso de protección, frente a la amenaza, perturbación o afectación de los derechos fundamentales reconocidos como garantía constitucional.

Este importante reconocimiento constitucional, además requerirá un adecuado equilibrio en su interacción con otros derechos fundamentales, experiencia que ha sido resuelta en el ámbito europeo y que seguramente se replicará en Chile, mediante el desarrollo del principio de proporcionalidad, en el entendido de que al igual que como ocurre con otros derechos, la protección de datos debe ser abordada desde su perspectiva social, y por consiguiente podrá limitarse su ejercicio, si se configuran ciertos requisitos o condiciones.

Sobre este punto, aparece como esclarecedor, lo dispuesto en el artículo 8.2 de la Carta de Derechos Fundamentales de la Unión Europea (CDFUE), al señalar; “Estos datos se tratarán de modo leal, para fines concretos y sobre la base del consentimiento de la persona afectada o

[116] Así se consagra por ejemplo en la legislación chilena (Ley N° 19.628) en el artículo 4° inciso 5° que dispone; “No requiere autorización el tratamiento de datos personales que provengan o que se recolecten de fuentes accesibles al público, cuando sean de carácter económico, financiero, bancario o comercial, se contengan en listados relativos a una categoría de personas que se limiten a indicar antecedentes tales como la pertenencia del individuo a ese grupo, su profesión o actividad, sus títulos educativos, dirección o fecha de nacimiento, o sean necesarios para comunicaciones comerciales de respuesta directa o comercialización o venta directa de bienes o servicios”.

[117] Contreras, P. (2020), “El derecho a la protección de datos personales y el reconocimiento de la autodeterminación informativa en la Constitución chilena”, en *Revista de Estudios Constitucionales*, vol. 8, núm. 2, p.101.

en virtud de otro fundamento legítimo previsto por la ley. Toda persona tiene derecho a acceder a los datos recogidos que la conciernan y a obtener su rectificación".

En relación con el artículo 52.1 de la misma Carta, que dispone: "Cualquier limitación del ejercicio de los derechos y libertades reconocidos por la presente Carta deberá ser establecida por la ley y respetar el contenido esencial de dichos derechos y libertades. Dentro del respeto del principio de proporcionalidad, sólo podrán introducirse limitaciones cuando sean necesarias y respondan efectivamente a objetivos de interés general reconocidos por la Unión o a la necesidad de protección de los derechos y libertades de los demás".

En otras palabras, la limitación a los derechos estatuidos en la Carta, en este caso, el de la protección de datos, podrá ser limitado si se transgreden los presupuestos establecidos, esto es que los datos se traten de modo desleal, sin fines concretos o sin el consentimiento de la persona afectada. Y en todo caso cuando una ley así lo disponga, agregando para una plausible limitación, la ponderación que se sustente en el interés general.

Al respecto es posible advertir que la Constitución chilena también establece la posibilidad de afectación y limitación de los derechos fundamentales solo por ley[118], siempre y cuando no se afecte la esencia de estos, lo que como se comprenderá implica una eventual colisión entre tales derechos, la que también debe ser resuelta por la adecuada ponderación que hagan los órganos jurisdiccionales mediante la aplicación entre otros, del principio de proporcionalidad.

En definitiva, como se ha expuesto, resulta evidente la interrelación de la protección de datos con otros derechos o garantías, y de igual forma, este se constituye como un derecho autónomo e independiente, instituyéndose su contenido en un poder de disposición y de control sobre los datos de carácter personal, otorgando al titular la facultad de oponerse, permitir o establecer límites al acceso y uso de sus datos. Es, como ya se ha señalado, una autodeterminación informativa o una libertad informática reforzada, dotando a sus titulares de una cobertura jurídica frente a los riesgos o eventuales transgresiones que el tratamiento de datos personales implica para la dignidad de las personas.

El autocontrol o la decisión autónoma sobre el tratamiento de datos personales por su titular, con independencia de si la información se encuentra en esferas más o menos públicas o privadas, explica de mejor forma la independencia conceptual y normativa del derecho a la protección de datos de otros derechos como el derecho a la intimidad o del derecho al respeto y protección de la vida privada.

Por todo lo expuesto, y como profundizaremos a continuación, de manera preliminar es posible definir el derecho a la protección de datos como la facultad del individuo de tener control sobre su propia información y establecer los márgenes que configuran su vida privada y estructuran su identidad propia.

[118] Artículo 19 N° 26 de la Constitución de la República de Chile; "La Constitución asegura a todas las personas… la seguridad de que los preceptos legales que por mandato de la Constitución regulen o complementen las garantías que esta establece o que las limiten en los casos que ella lo autoriza, no podrán afectar los derechos en su esencia, ni imponer condiciones, tributos o requisitos que impidan su libre ejercicio".

Aproximación al Derecho a la Protección de Datos a nivel internacional

Como se ha señalado, no solo la jurisprudencia si no también la doctrina se ha dado a la labor de conceptualizar y determinar el contenido del derecho a la protección de datos personales. Murillo se refiere a este derecho como aquel "control que ofrece a las personas sobre el uso por terceros de información sobre ellas mismas"[119], y Piñar Mañas explica que es "la facultad del individuo de decidir básicamente por sí solo sobre la difusión y utilización de sus datos personales"[120]. Esto implica el control del titular de los datos sobre dichos datos, lo que es expresión del libre desarrollo de su personalidad, en los mismos términos que lo explican las sentencias del Tribunal Constitucional Federal alemán, revisadas anteriormente. Por lo que la concepción constitucional de la dignidad entendida en su dimensión de autonomía obliga al Estado a tratar a los miembros de la comunidad como personas capaces de autodeterminarse, entre otros aspectos, en lo que se refiere al uso de su información personal.

Antecedentes al Derecho a la Protección de Datos

De las diversas fuentes bibliográficas consultadas, es posible concluir que ya en la antigua Grecia existía interés por mantener la confidencialidad sobre ciertas acciones y actividades realizadas por el hombre. Expresión de ello es el juramento Hipocrático (Grecia 460-377 a. c.), el cual se mantiene vigente hasta nuestros días: "… de todo aquello que vea u oiga en la sociedad durante el ejercicio de mi profesión, e incluso fuera de él, callaré lo que no necesite ser nunca divulgado, considerando la discreción como un deber en semejante caso"[121].

También en el ámbito clerical, es posible distinguir la importancia de la reserva o confidencialidad, en el denominado secreto de confesión, que impone a los sacerdotes el deber de guardar el secreto sacramental al señalar: "Procure con todo cuidado no delatar en lo más mínimo al pecador, ni por palabra, ni por signo, ni por cualquier otro modo… por que quien intentare revelar el pecado que le ha sido manifestado en el juicio de la penitencia, será entregado a hacer penitencia perpetua en un monasterio apartado"[122].

Como ya señalamos en líneas anteriores, en el espacio europeo el Convenio Europeo de Derechos Humanos (CEDH), suscrito en Roma el 4 de noviembre de 1950, en su artículo 8 reconoce el derecho al respeto a la vida privada y familiar. Posteriormente, en 1967, el Consejo de Europa crea una Comisión Consultiva para estudiar los riesgos que las tecnologías de la información generan sobre los derechos de las personas. Como consecuencia de dicha

---

[119] Murillo de la Cueva, P. (2009), "La construcción del derecho a la autodeterminación informativa y las garantías para su efectividad", en Murillo de la Cueva, Pablo Lucas y Piñar Mañas, J. L., "*EL Derecho a la Autodeterminación Informativa*", Madrid, Fundación Coloquio Europeo, p.11.

[120] Piñar Mañas, J. L. (2009), "Protección de Datos: Origen, situación actual y retos de futuro", en Murillo de la Cueva, Pablo Lucas y Piñar Mañas, J. L., *EL Derecho a la Autodeterminación Informativa*. Madrid, Fundación Coloquio Europeo, p.89.

[121] Becher, J. (2004), "El individuo, las tecnologías de la información y los medios de comunicación de masas", en *Historia de la Humanidad, El Siglo XX. La Globalización de las culturas*, Editorial Planeta, pp.654-657.

[122] Rodríguez Molina, J. (2008) "La confesión auricular. Origen y desarrollo histórico", *Gazeta de Antropología*, 24 (1), enero-junio puede consultarse en: http://www.ugr.es/~pwlac/G24_11Jose_Rodriguez_Molina.html

comisión, en el año 1968 se dicta la Resolución 509 sobre los derechos humanos y los nuevos logros científicos y técnicos, en la que se resalta la necesidad de la protección de la privacidad frente al surgimiento de las nuevas tecnologías[123].

Directrices de la OCDE de 1980

Por su parte, la Organización para la Cooperación y el Desarrollo Económico, (OCDE), el 23 de septiembre de 1980 aprueba una recomendación que contiene las "Directrices relativas a la protección de la privacidad y flujos transfronterizos de datos personales"[124].

Este documento aborda la forma en que deben ser procesados los datos, el contexto en que se utilizan, así como la naturaleza de estos, conceptualizándolos en la Primera parte 1. Letra b) de las directrices como "toda información relacionada con un individuo identificado o identificable" independientemente de si su procesamiento o tratamiento se lleva a cabo en el sector público o privado, o si se hace de forma automática o manual. También consagra ocho principios para ser aplicados a nivel nacional, específicamente en su "Parte Segunda: Principios Básicos de Aplicación Nacional"[125]:

1. Principio de limitación de recogida

Debería haber límites a la recogida de datos personales y cualquiera de esos datos debería ser obtenido por medios legales y honestos y, en su caso, con el conocimiento o consentimiento del sujeto de los datos.

2. Principio de calidad de los datos

Los datos personales deberían corresponder a los fines para los que se van a usar y, en la medida en que sean necesarios para esos fines, deberían ser correctos y completos, y estar actualizados.

---

[123] La preocupación del Consejo de Europa en esta materia puede considerarse pionera en el ámbito de las organizaciones internacionales. Puede Consultarse en: http://www.iepala.es/curso_ddhh/ddhh549.htm. Así, es posible distinguir una serie de fases o momentos en el sistema del Consejo de Europa, a la hora de proteger los Derechos Humanos, especialmente el derecho a la intimidad, frente a los nuevos avances tecnológicos. Esos momentos se pueden sintetizar en seis: 1) Creación en el año de 1967 de una Comisión Consultiva para estudiar el impacto de las nuevas tecnologías en el ámbito de los Derechos Humanos; 2) La resolución 509 de la Asamblea del Consejo de Europa, adoptada en el año 1968, sobre "los Derechos Humanos y los nuevos logros científicos y técnicos"; 3) En el año 1971 el Comité de Ministros designa una comisión de expertos, encargada de elaborar proyectos para la tutela de las libertades, en especial del derecho a la intimidad, frente a los avances tecnológicos; 4) Resolución del Comité de Ministros de 26 de Septiembre de 1973, relativa a "La protección de la vida privada de las personas físicas frente a los bancos de datos electrónicos en el sector privado"; 5) Resolución de 20 de Septiembre de 1974 relativa a "la protección de la vida privada de las personas físicas frente a los bancos de datos electrónicos en el sector público"; 6) Resolución del Comité de Ministros de 1976 por la que se crea una comisión de expertos encargada de desarrollar los trabajos preparatorios de lo que será un futuro Convenio sobre la materia; 7) Elaboración y aprobación el 28 de Enero de 1981 del Convenio Europeo sobre Protección de Datos Personales. El convenio presenta como características de mayor interés las siguientes.

[124] Consulta realizada el 17 de abril de 2020 en: https://www.oecd.org/sti/ieconomy/15590267.pdf

[125] Ver http://www.oas.org/es/sla/ddi/docs/Directrices_OCDE_privacidad.pdf, consulta efectuada el 17 de abril de 2010.

3. Principio de especificación de los fines

Los fines para los que los datos personales se recogen deberían especificarse en el momento en que se recogen, y su uso posterior estaría limitado al cumplimiento de esos fines o de otros que no sean incompatibles con esos fines y se especifiquen cada vez que haya un cambio de los mismos.

4. Principio de limitación de uso

Los datos personales no se deberían revelar, poner a disposición del público ni usar para fines que no sean los especificados, excepto: a) con el consentimiento del sujeto de los datos; o b) por imperativo legal.

5. Principio de salvaguarda de la seguridad

Los datos personales deberían estar protegidos por las oportunas medidas de salvaguarda contra riesgos como pérdida o acceso no autorizado, destrucción, uso, modificación o revelación de datos.

6. Principio de transparencia

Debería haber una política general de transparencia en lo concerniente al tratamiento, el uso y las políticas relativas a los datos personales. Se deberían poner los medios para establecer la existencia y la naturaleza de los datos personales, así como los fines principales para los que se van a usar, como la identidad y el domicilio habitual del inspector de datos.

7. Principio de participación individual

Este principio implica que toda persona física debería tener derecho a:

a) Conseguir, a través de un inspector de datos o de otra manera, la confirmación de si el inspector tiene o no tiene datos relativos a su persona;

b) Que se le comunique cualquier dato relativo a ella:

- ✓ en un plazo de tiempo razonable
- ✓ con una tarifa, en su caso, que no sea excesiva
- ✓ de manera razonable
- ✓ y de forma que pueda entender fácilmente

c) Que se le den las razones de por qué se rechaza una petición hecha de conformidad con lo establecido en los apartados (a) y (b), y poder recurrir de ese rechazo;

d) Recusar los datos relativos a ella y, si la recusación tiene éxito, hacer que se eliminen, rectifiquen, completen o modifiquen los datos.

8. Principio de responsabilidad

A todo inspector de datos se le deberían pedir responsabilidades por el cumplimiento de las

medidas que permiten la aplicación de los principios antes expuestos.

El Derecho a la protección de datos en Europa y Latinoamérica

La protección de datos, en el marco de la tradición jurídica de Europa continental, surge paralelamente con el desarrollo de la computación y el tratamiento de la información[126]. La primera respuesta relevante a la potencial amenaza de la informática en la vida privada de las personas, que impulsó la creación de normas específicas que rigieran la recolección y el tratamiento de información personal, se presenta en 1968 cuando las autoridades del *Land de Hesse* (Alemania), deciden aumentar la eficiencia de la administración pública mediante la automatización de los procesos, para lo cual se designó una comisión ad hoc. Dos años más tarde se crea la Unión de Procesamiento de Datos de Hesse, la Central de Hesse para Procesamiento de Datos y tres centros de cómputos regionales, con lo que dicho Estado y su administración comunal configuraron la primera infraestructura que unió la información y la comunicación.

Esta modernización regional llegó acompañada de ciertos resguardos normativos, por cuanto se sospechaba que la recolección y almacenamiento de datos podrían constituir una amenaza para los ciudadanos, como respuesta a ello se dicta la Ley de protección de datos del *Land* de Hesse, primer cuerpo normativo en el mundo en regular los datos personales en poder de los órganos públicos. De igual forma, también en Alemania, en Renania – Palatinado, se optó por una ley específica contra el uso indebido de los datos de carácter personal[127].

Años más tarde se dictaría en Suecia, en 1973, la primera ley con alcance nacional en regular la protección de datos personales. Sobre este punto hay que considerar que el ordenamiento jurídico de ese país entrega una prevalencia a la transparencia y a la publicidad, por lo que esta primera legislación tenía por finalidad prevenir invasiones indebidas y proteger la integridad personal. Esta ley reguló el procesamiento automatizado de datos, mediante un estatuto especial, de igual forma estableció una nueva autoridad de control para la protección de datos y estableció mecanismos de registro y licencias previas.

Con posterioridad a la normativa del *Land Hesse,* Alemania también establece su primera ley nacional sobre protección de datos en el año 1977, legislación que por primera vez puso el foco en el procesamiento de datos en el sector privado, basándose en el principio de prohibición general de tratamientos de datos de carácter personal salvo que la ley lo autorizara o existiera consentimiento del titular de dichos datos.

Por su parte Francia, en 1978 dicta su primera legislación en materia de protección de datos con la finalidad de que los adelantos tecnológicos no afectaran derechos fundamentales, tales como la dignidad humana, las libertades individuales y la vida privada. En la legislación

[126] Al revisar la historia de las nuevas tecnologías, se comprueba que durante la década de los sesenta del siglo XX el desarrollo de la informática impulsó el tratamiento de los datos en grandes cantidades, fenómeno que se acentuaría en los años setenta. Véase: Fernández-Izquierdo, F. (2000), "La historia moderna y las nuevas tecnologías de la información y las comunicaciones", en *Cuadernos de Historia Moderna* (vol. 24), p.209.

[127] Se establecieron normas generales para la protección de datos y derechos de las personas afectadas por información incorrectamente almacenada, aplicadas al sector público. Véase: Gonzalez Fuster, G. (2015), "*The Emergence of Personal Data Protection as a Fundamental Rigth of the EU"*, Bruselas, Springer, p.57.

francesa se disponía la definición de datos personales como aquellos directa o indirectamente identificables, esto es, aquellos datos que, sin estar asociados al nombre de una persona, pueden ser utilizados fácilmente para individualizarla y conocer sus hábitos y gustos[128].

Legislaciones similares a las descritas desarrollaron países como Dinamarca, Noruega y Luxemburgo, sobre datos personales tanto de aquellos registrados y almacenados por entidades privadas como por las respectivas administraciones públicas.

A su vez Portugal, España y Austria regularon la protección de datos a nivel constitucional o elevaron a rango constitucional legislaciones existentes. Portugal en su Constitución de 1976, artículo 35[129] inciso primero dispone: "Todos los ciudadanos tienen derecho a formar conocimiento de todo aquello que les concierna y se halla en registros informáticos y la finalidad para la cual se destinan las informaciones, de conformidad con lo dispuesto en la ley".

Regulando en dicho precepto de manera muy completa, la utilización de la informática y su afectación al derecho de protección de datos, prohibiendo el tratamiento y uso de ciertos datos cuando hagan inidentificable a un individuo, remitiendo además a la legislación la conceptualización y regulación de la noción de "dato personal".

El caso español, que analizaremos en las siguientes líneas con mayor profundidad, introdujo a nivel constitucional en el artículo 18.4[130] un apartado relacionado con la limitación al uso de las tecnologías de la información y comunicación (TIC), con el propósito de asegurar el honor de los ciudadanos y su intimidad personal y familiar.

Si bien la Constitución española no consagra expresamente el derecho a la protección de datos personales, mandata al legislador para regular el uso de la informática, con lo que el Tribunal

---

[128] Phillipe, J. y Guyon, A.-Ch. (2015), "Data protection in France: overview", *Practical Law Association of Corporate Council*, Global Guide 2015/2016 Data Protection (Country QUA), pp.1-9.

[129]Artículo 35: Utilización de la Informática "Todo ciudadano tendrá derecho de acceso a todos los registros informáticos que le conciernen, a requerir que sean rectificados y actualizados, y a ser informado de la finalidad a que se destinan las informaciones, de conformidad con lo dispuesto en la ley.

La ley definirá el concepto de "dato personal", junto con términos y condiciones aplicables a su tratamiento automatizado, vínculos, transmisiones y uso, y garantizará su protección, en particular por medio de un órgano independiente.

No se podrá utilizar la informática para el tratamiento de datos referentes a convicciones filosóficas o políticas, afiliaciones a partidos o sindicatos, creencias religiosas, vida privada u orígenes étnicos, salvo con el consentimiento expreso del sujeto, con autorización prevista por la ley y garantías de no discriminación, o con el fin de procesar datos estadísticos que no puedan ser individualmente identificados.

El acceso de terceros a los datos personales estará prohibido, salvo en casos excepcionales, de conformidad con la ley.

Se prohíbe atribuir un número nacional único a los ciudadanos.

Se garantiza a todos el libre acceso a la red informática de uso público. La ley determinará tanto las reglas aplicables al flujo de datos a través de las fronteras como las medidas apropiadas para proteger datos personales y otros que justificadamente hayan de ser salvaguardados en interés nacional.

Los datos personales contenidos en archivos manuales disfrutarán de la misma protección prevista en los apartados precedentes, de conformidad con lo dispuesto en la ley".

[130] "La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de los derechos".

Constitucional Español ha reconocido la existencia de la protección de datos personales, como un derecho independiente y autónomo, diferente a la intimidad personal y a la vida privada[131].

Austria incluyó en su ley de protección de datos[132] un apartado en el que se le otorga a este derecho fuerza y tutela, siendo el primer país en consagrar este derecho protegido constitucionalmente, sin embargo, como señala Martínez López-Sáez[133], "no lo consideraba ni independiente ni autónomo, sino intrínsecamente ligado al derecho al respeto de la vida privada y familiar". En la actualidad la Constitución austríaca consagra en su apartado primero: "Toda persona tiene derecho al secreto de sus datos personales, especialmente en lo que se refiere a su vida privada y familiar, si hay un interés legítimo. Se descarta la existencia de tal derecho si los datos están disponibles en general o si no se puede rastrear la procedencia de los datos del individuo afectado". Reconociendo en términos explícitos e inequívocos la protección de datos como un derecho fundamental.

Los otros países de Europa siguieron con el desarrollo normativo de la protección de datos, influenciados también por las regulaciones a través de instrumentos internacionales promovidos por organismos como la Organización para la Cooperación y Desarrollo Económico, OCDE y el Convenio N° 108 del Consejo de Europa, de 28 de enero de 1981, para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, el que entró en vigencia en 1985 y que tiene la particularidad de ser un tratado abierto a la firma de cualquier Estado y no solo a los Estados miembros del Consejo de Europa. A la fecha ha sido suscrito solo por tres Estados latinoamericanos, que incluyen a Argentina, México y Uruguay[134].

Como señala Cazurro Barahona[135], si bien el Convenio 108 es el principal hito que se debe tener en cuenta, el Consejo de Europa ya había querido regular el tratamiento de la información personal a través de otros mecanismos. En este contexto, en 1967 la Asamblea Parlamentaria del Consejo de Europa dirigió al Comité de Ministros la Recomendación 509, de 31 de enero de 1967, de la Asamblea Parlamentaria del Consejo de Europa, sobre los derechos humanos y los nuevos logros científicos y técnicos. En ella, al estudiar las nuevas tecnologías de la información y el potencial peligro de estas para los derechos personales, se puso en evidencia la escaza e insuficiente protección que las diferentes legislaciones nacionales prestan al derecho a la vida privada del individuo en relación con el tratamiento automatizado de datos personales. Ante este escenario, el Comité de Ministros del Consejo de Europa designará una

---

[131] Ver sentencias 254/1993 de 20 de julio y 292/2000 de 30 de noviembre, en las que el Tribunal aborda la protección de datos personales como un derecho fundamental autónomo de la intimidad y más amplio para evitar potenciales agresiones a la dignidad y libertad personal, proveniente de un uso ilegitimo del tratamiento mecanizado de datos a través de un mayor control de los datos personales, entendidos aquellos que identifican o hacen identificable a la persona.

[132] Bundesgesetz über den Schutz personenbezogener Daten – Datenschutzgesetz- DSG-Ley de Protección de Datos personales de 18 de octubre de 1978, nº 565.

[133] Martínez López-Sáez, M. (2018) "Una revisión al derecho fundamental a la protección de datos de carácter personal", Tirant Lo Blanch, Valencia, pp.63-64.

[134] Los Estados firmantes pueden revisarse en la web en: https://www.coe.int/en/web/conventions/full-list/-/conventions/108/signatures?p_auth=SWNsnUpq

[135] Cazurro Barahona, V. (2020) "*Antecedentes y Fundamentos del Derecho a la Protección de Datos*", Boch Editor, Barcelona, p.83.

Comisión Intergubernamental de expertos encargada de elaborar una serie de proyectos para la tutela de las libertades, y especialmente, para la tutela de la intimidad, frente a los peligros derivados de los avances tecnológicos. Fruto del trabajo de esta Comisión fueron la Resolución 73/22 de 26 de septiembre de 1973, sobre la protección de la vida privada de las personas físicas respecto de los bancos de datos electrónicos en el sector privado; y la Resolución 74/29, de 20 de septiembre de 1974, sobre la protección de la vida privada de las personas físicas respecto de los bancos de datos electrónicos en el sector público[136].

Estas Resoluciones son especialmente relevantes, ya que constituyen el primer texto europeo supranacional en los que se recogen principios básicos, algunos vigentes hasta hoy, del tratamiento de datos de carácter personal, tales como el principio de lealtad, el principio de finalidad, el principio de exactitud, el derecho a ser informado, el derecho de acceso, el derecho de confidencialidad y el derecho de seguridad del tratamiento.

Siguiendo en el contexto europeo, la sentencia del Tribunal Constitucional alemán de 1982, que recogió la denominada teoría de las tres esferas de Hubmann[137], explicada en páginas anteriores, vincula la protección de datos con los atributos derivados de la dignidad de la persona, pudiendo esta prohibir o limitar la recogida, almacenamiento, utilización y difusión ilimitada de sus datos, como igualmente disponer libremente de estos, de ahí la denominación de autodeterminación informativa a la que hace referencia el derecho alemán. Estableciendo la señalada sentencia la vulneración que implica para el titular de los datos, el tratamiento de estos sin adecuados mecanismos de garantía. Señala la STC alemán a este respecto:

"El que no puedas percibir con seguridad suficiente que informaciones relativas a él son conocidas en determinados sectores de su entorno social y quien de alguna manera no sea capaza de aquilatar lo que puedan saber de él sus posibles comunicantes puede verse sustancialmente cohibido en su libertad de planificar o decidir por autodeterminación… Quien se siente inseguro de si en todo momento por que se registra cualquier comportamiento divergente y se cataloga, utiliza o transmite permanentemente a título de información procurará no llamar la atención con esa clase de comportamiento. Quien sepa de antemano que su participación, por ejemplo, en una reunión o iniciativa cívica va a ser registrada por las autoridades y que podrán derivarse riesgos para él por este motivo renunciará presumiblemente a lo que se supone un ejercicio de los correspondientes derechos fundamentales".

En el ámbito latinoamericano, la normativa sobre protección de datos no es uniforme y da cuenta de una diversidad y dispersión normativa; en efecto, mientras algunas legislaciones regulan la materia de manera específica otras no tienen regulación alguna o están en vías de aquello. En este sentido algunos países consagran la protección de datos personales como un derecho fundamental estatuido en sus respectivas constituciones y otros, en cambio, solo lo abordan a nivel legislativo. Repasaremos solo como corolario inicial el tratamiento que a la protección de datos le dan los ordenamientos jurídicos de Colombia, Perú y México.

---

[136] Ver en: http://www.informatica-juridica.com/legislacion/union-europea/, consulta realizada el 16 de septiembre de 2021.

[137] Hubmann, H. (1967), "*Das Personlichkeitsrecht*", Colonia, 2° edición, , pp.268 y ss.; Seidel, U. (1974), "*Datenbanken und Datenschutz*", Frankfurt, p.65.

El Derecho a la Protección de Datos en Colombia

Colombia, en su Constitución de 1991, que reemplazó a la Carta Política de 1886, incorporó de manera expresa el derecho de toda persona de conocer, actualizar y rectificar las informaciones que se hayan recogido de bases de datos, derecho garantizado constitucionalmente y por consiguiente resguardado por la Corte Constitucional a través de la denominada acción de tutela, que estableció los principios y parámetros del habeas data.[138] Pero no fue sino hasta el año 2008, con la dictación de la Ley N° 1266 que se regula a nivel legislativo el tratamiento de datos personales, eso sí solo enfocado en aspectos crediticios y financieros, sin embargo, el señalado precepto estableció avances significativos al crear las figuras de operador de datos y fuentes de información, asignándole deberes y responsabilidades, estableciendo un procedimiento expedito para reclamos y determinando cuatro grandes categorías de datos en función de su contenido y naturaleza: datos públicos, datos semiprivados, datos privados y datos sensible[139].

Luego, en el año 2012 se dicta el Ley N° 1581, ley de rango estatutario (superior a la ley ordinaria) que consagra el régimen general de protección de datos aplicable a todos los sectores de la economía incluyendo los datos gestionados por el sector público.

Destaca en esta legislación la incorporación del principio de responsabilidad demostrada, en virtud del cual la entidad responsable tiene la obligación de implementar las medidas preventivas suficientes para ofrecer una adecuada protección de los derechos de los titulares, en relación con su tamaño e incidencia.

A continuación, en el año 2013, se dicta el Decreto 1377, que aterriza la Ley N° 1581 reglamentando cuestiones relacionadas con el consentimiento del titular de los datos, el tratamiento de los responsables y encargados de los datos, así como la transferencia de los datos personales, entre otras materias.

---

[138] El artículo 15 de la Constitución colombiana señala: "Todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, y el Estado debe respetarlos y hacerlos respetar. De igual modo, tienen derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos y en archivos de entidades públicas y privadas.

En la recolección, tratamiento y circulación de datos se respetarán la libertad y demás garantías consagradas en la Constitución.

La correspondencia y demás formas de comunicación privada son inviolables. Solo pueden ser interceptadas o registradas mediante orden judicial, en los casos y con las formalidades que establezca la ley.

Para efectos tributarios o judiciales y para los casos de inspección, vigilancia e intervención del Estado podrá exigirse la presentación de libros de contabilidad y demás documentos privados, en los términos que señale la ley".

[139] La señalada ley, dispuso que los datos de contenido crediticio y financiero correspondían a la categoría de datos semiprivados, los cuales pueden ser recogidos de forma automatizada, pero siempre con autorización previa y expresa del titular de estos.

El Derecho a la Protección de Datos en Perú

Según lo dispuesto en el artículo dos del numeral sexto de la Constitución Política del Perú, toda persona tiene derecho a que los servicios informáticos, computarizados o no, públicos o privados, no suministren informaciones que afecten la intimidad personal y familiar[140].

Sobre este antecedente constitucional, el 21 de junio de 2011 se aprueba la Ley de Protección de Datos Personales N° 29.733, que dispone un conjunto de derechos y obligaciones que regulan la materia en Perú. Luego, el 21 de marzo de 2013 se aprueba mediante Decreto Supremo 003-2013-JUS, su respectivo reglamento, los que fueron actualizados por el Decreto Legislativo N° 1.353 del año 2017 que reformó aspectos relacionados con el régimen de la protección de datos en dicho país, creando la Autoridad de Transparencia y Acceso a la Información Pública, fortaleciendo el régimen de protección de datos personales y la regulación de la gestión de intereses.

La precedente normativa peruana, (artículo 3 de la ley y artículo 5 del reglamento), circunscribe el ámbito de aplicación al tratamiento de datos personales contenidos en bases privadas como de la administración pública, cuando el tratamiento de los datos se realiza en el territorio nacional.

Un aspecto para destacar de la regulación peruana es que la creación, modificación o cancelación de bancos de datos personales se debe inscribir en el Registro Nacional de Protección de Datos Personales a cargo de la Autoridad de Protección de Datos. Este registro de naturaleza administrativa tiene por finalidad inscribir en forma diferenciada a nivel nacional: i) Los bancos de datos personales de administraciones públicas o privadas; ii) Los códigos de conducta; iii) Las sanciones, medidas cautelares o correctivas impuestas por la autoridad y iv) Las comunicaciones referidas al flujo transfronterizo de datos personales.

Este registro persigue dar publicidad a la inscripción de los bancos de datos personales pudiendo ser consultados por cualquier persona.

El Derecho a la Protección de Datos en México

En México, la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, vigente desde el 6 de julio de 2010 y su respectivo Reglamento, en vigencia desde el 22 de abril del año 2011, son las principales fuentes jurídicas que tienen por objeto regular el tratamiento legítimo, controlado e informado de los datos personales, para garantizar la privacidad y el derecho a la autodeterminación informativa de las personas.

En México, la protección de datos personales está establecida en el artículo 16[141] de la Constitución Política de los Estados Unidos Mexicanos que establece que toda persona tiene

[140] El artículo 2° numeral 6 de la Constitución del Perú señala*:* "Toda persona tiene derecho: A que los servicios informáticos, computarizados o no, públicos o privados, no suministren informaciones que afecten la intimidad personal y familiar."

[141] En lo pertinente, el artículo 16 de la Constitución Mexicana dispone en su inciso 2°: "Toda persona tiene derecho a la protección de sus datos personales, al acceso, rectificación y cancelación de los mismos, así como a manifestar su oposición, en los términos que fije la ley, la cual establecerá los supuestos de excepción a los

derecho a la protección de sus datos personales, al acceso, rectificación y cancelación de estos, así como a manifestar su oposición, en los términos que fije la ley. La Constitución impone obligaciones a las personas físicas o jurídicas que utilizan datos personales y le otorga el derecho a toda persona física de decidir quién puede tratar sus datos personales y para qué fines.

El Estado Mexicano suscribió y ratificó diversos tratados internacionales relacionados con la protección de datos, incluyendo el Convenio para la Protección de las Personas con respecto al Tratamiento Automatizado de Datos de Carácter Personal, celebrado en Estrasburgo, Francia, el 28 de enero de 1981, así como el Protocolo Adicional de fecha 8 de noviembre de 2001, los cuales entraron en vigor en México el 1° de octubre de 2018.

En los últimos años, los órganos legislativos, tanto federal como de diversos Estados de la República Mexicana, han expedido leyes en materia de protección de datos en posesión de cualquier autoridad, entidad, órgano y organismos de los poderes Ejecutivo, Legislativo y Judicial, órganos autónomos, partidos políticos, fideicomisos y fondos públicos, de la Federación, los Estados y los municipios, con la finalidad de regular su adecuado tratamiento.

De conformidad a la normativa mexicana, específicamente el artículo 3 V, los datos personales son: “Cualquier información concerniente a una persona física identificada o identificable” y según el mismo artículo 3 VI, datos personales sensibles son “Aquellos datos personales que afecten a la esfera más íntima de su titular, o cuya utilización indebida pueda dar origen a discriminación o conlleve un riesgo grave para este. En particular, se consideran sensibles aquellos que puedan revelar aspectos como origen racial o étnico, estado de salud presente y futuro, información genética, creencias religiosas, filosóficas y morales, afiliación sindical, opiniones políticas, preferencia sexual”.

Un aspecto a destacar en la regulación de la protección de datos personales en México y sobre el cual profundizaremos, dice relación con la autoridad de control en la materia, en efecto, el órgano encargado de verificar el cumplimiento de la normativa sobre protección de datos es el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos – INAI, que como su nombre lo indica verifica y regula no solo la protección de datos si no también el acceso a la información pública, es decir, dos derechos que interactúan entre sí. El INAI es un órgano autónomo constitucional, es decir tiene independencia de los poderes públicos (ejecutivo, legislativo y judicial) y goza de independencia funcional y financiera.

El Derecho a la Protección de Datos en Chile

El 28 de agosto de 1999 se publica en el Diario Oficial chileno la Ley N° 19.628 sobre protección a la vida privada[142], también conocida como ley de protección de datos personales. Esta se estructura en un título preliminar, cinco títulos y un título final, el título preliminar se refiere a las disposiciones generales al objeto de la ley, sus límites, así como la definición de ciertas y determinadas palabras; el título primero se refiere a la utilización de los datos

principios que rijan el tratamiento de datos, por razones de seguridad nacional, disposiciones de orden público, seguridad y salud públicas o para proteger los derechos de terceros”.

[142] Como se puede apreciar, el título de la ley limita la protección de datos a la vida privada y no reconoce, el legislador de la época, seguramente de manera involuntaria, la autonomía e independencia de este derecho.

personales y principalmente aborda los principios en que se sustenta la protección de datos personales que tienen por finalidad resguardar su adecuado tratamiento; en el título segundo se abordan los derechos de los titulares de datos, donde se distingue entre los derechos de acceso, rectificación, cancelación y bloqueo; el título tercero hace referencia a la utilización de datos personales relativos a obligaciones de carácter económico; el título cuarto se refiere al tratamiento de datos por los organismos públicos; el título quinto aborda la responsabilidades generadas por las infracciones a la ley y por último el título final se refiere en un solo artículo, el 24, al introducir una modificación al Código Sanitario Chileno, otorgándole la calidad de reservados a las recetas médicas, exámenes de laboratorios y servicios relacionados con la salud en general[143].

Como se señaló, el artículo 1 del título primero establece su objeto y determina sus límites; "Artículo 1º.- El tratamiento de los datos de carácter personal en registros o bancos de datos por organismos públicos o por particulares se sujetará a las disposiciones de esta ley, con excepción del que se efectúe en ejercicio de las libertades de emitir opinión y de informar, el que se regulará por la ley a que se refiere el artículo 19 N° 12, de la Constitución Política.

Toda persona puede efectuar el tratamiento de datos personales, siempre que lo haga de manera concordante con esta ley y para finalidades permitidas por el ordenamiento jurídico. En todo caso deberá respetar el pleno ejercicio de los derechos fundamentales de los titulares de los datos y de las facultades que esta ley les reconoce".

La finalidad de esta ley es tutelar la información relativa a personas naturales, garantizando que, en definitiva, sean ellas las que decidan sobre su uso o tratamiento.

Se podría decir que la ley chilena, con casi tres décadas de diferencia, fue heredera de una serie de iniciativas legislativas provenientes principalmente de Europa, en la que diversos países a finales de la década del sesenta y durante la década del setenta empezaron a dictar leyes que regularon la protección de los datos personales, iniciativas legislativas que evidentemente fueron detrás del vertiginoso desarrollo informático y tecnológico. Lo que Pérez Luño denomino "la generación de leyes de protección de datos personales" [144].

En este mismo sentido, "nuestra ley no es sino eco de las leyes de protección de datos que aparecieron en el último medio siglo de la mano del creciente desarrollo de la informática, el

[143] Artículo 24: "Agrégase los siguientes incisos segundo y tercero, nuevos, al artículo 127 del Código Sanitario: "Las recetas médicas y análisis o exámenes de laboratorios clínicos y servicios relacionados con la salud son reservados. Sólo podrá revelarse su contenido o darse copia de ellos con el consentimiento expreso del paciente, otorgado por escrito. Quien divulgare su contenido indebidamente, o infringiere las disposiciones del inciso siguiente, será castigado en la forma y con las sanciones establecidas en el Libro Décimo. Lo dispuesto en este artículo no obsta para que las farmacias puedan dar a conocer, para fines estadísticos, las ventas de productos farmacéuticos de cualquier naturaleza, incluyendo la denominación y cantidad de ellos. En ningún caso la información que proporcionen las farmacias consignará el nombre de los pacientes destinatarios de las recetas, ni el de los médicos que las expidieron, ni datos que sirvan para identificarlos".

[144] Pérez Luño, A. (1989) "*Los derechos humanos en la sociedad informática*", Centro de Estudios Constitucionales, Madrid, pp.133-185.

que ha permitido procesar datos de una manera que antes era completamente inconcebible y que desde el advenimiento de internet permite transferirlos con enorme facilidad"[145].

El artículo segundo letra f) de la ley, conceptualiza los datos personales como "Datos de carácter personal o datos personales, los relativos a cualquier información concerniente a personas naturales, identificadas o identificables". Es decir, aquellos datos que permiten individualizar a una persona, determinado quién es el titular de los mismos, y que la propia ley se encarga de diferenciar de los datos estadísticos que son aquellos que "en su origen, o como consecuencia de su tratamiento, no puede ser asociado a un titular identificado o identificable"[146].

La ley también define, ahora en la letra g) del señalado artículo dos, un tipo de datos que requieren mayor tutela y protección, son los datos sensibles, "aquellos datos personales que se refieren a las características físicas o morales de las personas o a hechos o circunstancias de su vida privada o intimidad, tales como los hábitos personales, el origen racial, las ideologías y opiniones políticas, las creencias o convicciones religiosas, los estados de salud físicos o psíquicos y la vida sexual".

La ley chilena, al igual que otros ordenamientos jurídicos, consagra una serie de principios para la protección de datos personales y su adecuada tutela y tratamiento, los cuales son posibles de sistematizar de la siguiente manera[147]:

a) El principio de licitud que se desprende de los artículos 2º, 4º incisos 1º[148] y 6º, según el cual el tratamiento solo cabe si existe autorización legal o de parte del titular, debiendo en este último caso tratarse de un consentimiento expreso, es decir que se manifieste en términos explícitos e inequívocos.

b) El principio de información al titular respecto del propósito del almacenamiento de sus datos personales, es decir, para qué se almacenarán los datos y su posible comunicación al público, establecido en el artículo 4°, inc. 2º[149].

c) El principio de veracidad de los datos, que exige corregir los que sean erróneos, inexactos, equívocos o incompletos según se colige del artículo 6°, inc. 2°[150].

[145] Rajevic Mosler, E. (2011) "Protección de datos y transparencia en la administración pública chilena: Inevitable y deseable ponderación" en *Reflexiones sobre el uso y abuso de los Datos Personales en Chile*. Editorial UDP – Expansiva, Santiago, pp.137-157.

[146] Artículo 2° letra e) de la Ley N° 19.628

[147] Rajevic Mosler, E. (2011) "Protección de datos y transparencia en la administración pública chilena: Inevitable y deseable ponderación" en *Reflexiones sobre el uso y abuso de los Datos Personales en Chile*. Editorial UDP – Expansiva, Santiago, pp.137-157.

[148] Artículo 4° "El tratamiento de los datos personales solo puede efectuarse cuando esta ley u otras disposiciones legales lo autoricen o el titular consienta expresamente en ello".

[149] "La persona que autoriza debe ser debidamente informada respecto del propósito del almacenamiento de sus datos personales y su posible comunicación al público".

[150] "Han de ser modificados cuando sean erróneos, inexactos, equívocos o incompletos".

d) El principio de finalidad de los datos, que se desprende del artículo 9º[151], y en virtud del cual debe respetarse la finalidad para la que fueron recogidos los datos, de manera que exista una relación directa entre esa finalidad y el dato recabado.

e) El principio de seguridad de los datos, contemplado y cautelado en el artículo 11[152] y, tratándose de los órganos de la Administración regulado por el D.S. N° 83/2004, SEGPRES[153].

f) El principio de confidencialidad que se aplica cuando se trata de datos obtenidos de fuentes no accesibles al público, según el artículo 7º[154].

Luego, el Título segundo y principalmente el artículo 12[155] de la ley hacen referencia a los derechos que se le confieren al titular, para salvaguardar el tratamiento de sus datos personales, como son los derechos de acceso, rectificación, cancelación y bloqueo[156]. Estos constituyen la contrapartida a la habilitación legal para el tratamiento de datos personales, contenida en el

---

[151] Artículo 9° inciso 1°: "Los datos personales deben utilizarse solo para los fines para los cuales hubieren sido recolectados, salvo que provengan o se hayan recolectado de fuentes accesibles al público".

[152] Artículo 11: "El responsable de los registros o bases donde se almacenen datos personales con posterioridad a su recolección deberá cuidar de ellos con la debida diligencia, haciéndose responsable de los daños".

[153] Este decreto del Ministerio Secretaría General de la Presidencia fue promulgado el 3 de junio del año 2004 y su título es "Aprueba norma técnica para los órganos de la Administración del Estado sobre seguridad y confidencialidad de los documentos electrónicos". Su objetivo es garantizar estándares mínimos de seguridad en el uso, almacenamiento, acceso y distribución del documento electrónico; además de facilitar la relación electrónica entre los órganos del Estado y entre éstos y la ciudadanía.

[154] Artículo 7°: "Las personas que trabajan en el tratamiento de datos personales, tanto en organismos públicos como privados, están obligadas a guardar secreto sobre los mismos, cuando provengan o hayan sido recolectados de fuentes no accesibles al público, como asimismo sobre los demás datos y antecedentes relacionados con el banco de datos, obligación que no cesa por haber terminado sus actividades en ese campo".

[155] Artículo 12: "Toda persona tiene derecho a exigir a quien sea responsable de un banco, que se dedique en forma pública o privada al tratamiento de datos personales, información sobre los datos relativos a su persona, su procedencia y destinatario, el propósito del almacenamiento y la individualización de las personas u organismos a los cuales sus datos son transmitidos regularmente.

En caso de que los datos personales sean erróneos, inexactos, equívocos o incompletos, y así se acredite, tendrá derecho a que se modifiquen.

Sin perjuicio de las excepciones legales, podrá, además, exigir que se eliminen, en caso de que su almacenamiento carezca de fundamento legal o cuando estuvieren caducos.

Igual exigencia de eliminación, o la de bloqueo de los datos, en su caso, podrá hacer cuando haya proporcionado voluntariamente sus datos personales o ellos se usen para comunicaciones comerciales y no desee continuar figurando en el registro respectivo, sea de modo definitivo o temporal.

En el caso de los incisos anteriores, la información, modificación o eliminación de los datos serán absolutamente gratuitas, debiendo proporcionarse, además, a solicitud del titular, copia del registro alterado en la parte pertinente. Si se efectuasen nuevas modificaciones o eliminaciones de datos, el titular podrá, asimismo, obtener sin costo copia del registro actualizado, siempre que haya transcurrido a lo menos seis meses desde la precedente oportunidad en que hizo uso de este derecho. El derecho a obtener copia gratuita sólo podrá ejercerse personalmente.

Si los datos personales cancelados o modificados hubieren sido comunicados previamente a personas determinadas o determinables, el responsable del banco de datos deberá avisarles a la brevedad posible la operación efectuada. Si no fuese posible determinar las personas a quienes se les hayan comunicado, pondrá un aviso que pueda ser de general conocimiento para quienes usen la información del banco de datos".

[156] Actualmente son los denominados derechos ARCO, acceso, rectificación, cancelación y oposición.

artículo 1º de la Ley 19.628. Por una parte, la ley permite a cualquiera realizar tratamiento de datos personales de un tercero, en la medida que cumpla con ciertos requisitos, y a su vez otorga herramientas que buscan asegurar que dichos datos se correspondan con la realidad y que el tratamiento cumpla con todos los requisitos legales. Por lo mismo, ante el caso de dejar de cumplirse cualquiera de estas dos condiciones, la ley garantiza a las personas el derecho a solicitar la modificación, cancelación o bloqueo de sus datos.

Luego, el artículo 13[157], dispone que los derechos de información, modificación, cancelación y bloqueo son indisponibles, no pudiendo ser limitados por medio de ningún acto o convención. A continuación, abordaremos cada uno de estos derechos, haciendo, donde sea posible[158], alguna referencia a su tratamiento en el actual Reglamento Europeo de Protección de Datos[159].

Derecho de acceso

Este derecho confiere al titular de datos personales la facultad de exigir al responsable del banco de datos que le entregue información sobre los datos relativos a su persona, su procedencia y destinatario, el propósito o finalidad del almacenamiento y la individualización de las personas u organismos a los cuales sus datos son transmitidos regularmente.

El RGPD, señala también a propósito de este derecho de acceso en su considerando 63, que: "Los interesados deben tener derecho a acceder a los datos personales recogidos que le conciernan y a ejercer dicho derecho con facilidad y a intervalos razonables, con el fin de conocer y verificar la licitud del tratamiento".

Autores como Aparicio Salom, plantean en relación con el derecho de acceso, que "es una de las manifestaciones esenciales del principio de transparencia y constituye uno de los elementos claves para la lealtad del tratamiento de los datos personales" [160].

Para concretar este derecho y hacerlo exigible, la ley establece la obligación a los organismos públicos de registrar las bases de datos en un registro público[161], a cargo del Registro Civil e Identificación[162]. Este registro público debe contener información acerca del fundamento jurídico de su existencia, su finalidad, tipos de datos almacenados y descripción del universo de personas que comprende. De manera inexplicable esta obligación no se ha hecho extensible a las entidades privadas, quedando estas últimas exentas de la obligación de registrar sus bases

[157] Artículo 13: "El derecho de las personas a la información, modificación, cancelación o bloqueo de sus datos personales no puede ser limitado por medio de ningún acto o convención".

[158] Por ejemplo, el RGPD regula el derecho al olvido y el derecho a la portabilidad, derechos que nos están regulados en la legislación chilena.

[159] Desde el día 25 de mayo de 2018 es aplicable el Reglamento de la Unión Europea 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y la libre circulación de estos datos y por el que se deroga la Directiva 95/46/EC.

[160] Aparicio Salom, J. (2018), "*Derechos del Interesado*" (artículos 12-19), El nuevo marco regulatorio derivado del Reglamento Europeo de Protección de Datos. Adaptado al Proyecto de Ley Orgánica de Protección de Datos de 10 de noviembre de 2017, coordinador José López Calvo, Boch, Barcelona, p.367.

[161] Ver: https://www.registrocivil.cl/principal/canal-tramites/banco-de-datos-personales

[162]Sobre este registro consultar: https://www.registrocivil.cl/principal/quienes-somos/terminos-y-condiciones-2

de datos, disminuyendo con ello la capacidad de las personas naturales de ejercer su derecho de información y acceso.

En el contexto iberoamericano, específicamente en lo relativo a los Principios Actualizados del Comité Jurídico Interamericano sobre la Privacidad y la Protección de datos Personales, con Anotaciones[163], el Principio número ocho se refiere al derecho de acceso, el cual supone que cada persona tenga la posibilidad de tener acceso a sus propios datos. En algunos casos, hasta terceros podrían tener derecho también, como ocurre con los representantes de personas con discapacidad mental o con los padres de menores.

Además, se establece que este derecho de acceso no es absoluto, ya que en todo sistema nacional hay situaciones excepcionales en las cuales se podría requerir que se mantenga el carácter confidencial de ciertos datos. Estas circunstancias deberían enunciarse claramente en las leyes apropiadas o en otras directrices y deberían ponerse a disposición del público[164].

Derecho a la modificación o rectificación[165]

Derecho consagrado en el artículo 2° letra j) de la Ley 19.628 como "todo cambio en el contenido de los datos almacenados en registros o bancos de datos". Este, faculta a su titular para corregir o integrar datos que consten de manera inexacta o incompleta en las respectivas bases. Otorgando la facultad al titular de los datos de solicitar su modificación, y la correlativa obligación del responsable del banco de datos de realizar dicha modificación, cuando estos sean erróneos, inexactos, equívocos o incompletos, y así se acredite.

Este derecho se relaciona con lo que algunos autores, como Murga Fernández, han denominado el principio de la exactitud[166], también vinculado a los principios de lealtad y transparencia al que hace referencia el RGPD[167].

---

[163] Ver en: CJI-doc_638-21.pdf (oas.org), consulta realizada el 18 de mayo de 2021.

[164] Por ejemplo, podrían surgir situaciones de ese tipo si se sospecha que la persona a la cual se refieren los datos ha cometido un acto ilícito y es el sujeto de una investigación que estén realizando las fuerzas del orden o una entidad similar, si los registros de esa persona están mezclados con los de un tercero que también tiene intereses en materia de privacidad o si otorgar acceso al titular de los datos podría comprometer secretos comerciales, pruebas confidenciales o material para exámenes. Las reglas relativas a situaciones de esos tipos deberían ser lo más estrechas y restrictivas posible.

[165] El artículo 16 el RGPD establece: "El interesado tendrá derecho a obtener sin dilación indebida del responsable del tratamiento la rectificación de los datos personales inexactos que le conciernan. Teniendo en cuenta los fines del tratamiento, el interesado tendrá derecho a que se completen los datos personales que sean incompletos, inclusive mediante una declaración adicional".

[166] Murga Fernández, J. (2017), "La protección de datos y los motores de búsqueda en internet: cuestiones actuales y perspectivas de futuro acerca del derecho al olvido", *Revista de Derecho Civil*, vol. IV, número 4, octubre-diciembre de 2017, pp.181-209.

[167] Dispone, el considerando 71 del RGPD: "… A fin de garantizar un tratamiento leal y transparente respecto del interesado, teniendo en cuenta las circunstancias y contexto específicos en los que se tratan los datos personales, el responsable del tratamiento debe utilizar procedimientos matemáticos o estadísticos adecuados para la elaboración de perfiles, aplicar medidas técnicas y organizativas apropiadas para garantizar, en particular, que se corrigen los factores que introducen inexactitudes en los datos personales y se reduce al máximo el riesgo de error, asegurar los datos personales de forma que se tengan en cuenta los posibles riesgos para los intereses y

La persona debería tener la posibilidad de ejercer el derecho a solicitar la corrección o la adición de datos personales sobre sí misma que sean incompletos, inexactos, innecesarios, excesivos o que no se encuentren actualizados. Si los Datos en cuestión son incompletos o inexactos, se debería permitir que la persona proporcione más información a fin de corregir los errores u omisiones.

Si los Datos en cuestión son evidentemente inexactos, el Responsable de estos, por lo general, deberá corregir la inexactitud cuando el titular de los datos lo solicite. Incluso en los casos en que se determine que los datos son inexactos, como en el curso de una investigación de su titular, a veces podría ser más apropiado que el Responsable agregue material al registro en vez de borrarlo, a fin de que refleje con exactitud la historia completa de la investigación.

El derecho de corrección o rectificación no es absoluto, por ejemplo, es posible que no se autorice la modificación de datos personales, aunque se trate de información errónea o engañosa, en los casos en que los datos se requieran legalmente o deban ser conservados para el cumplimiento de una obligación impuesta a la persona responsable por la ley nacional pertinente o posiblemente por las relaciones contractuales entre el responsable y el titular de los datos. Por consiguiente, en la legislación respectiva se deberían indicar claramente las condiciones en las cuales se deberá proporcionar acceso y permitir la corrección de los datos, así como las restricciones que se apliquen y, en tal caso, los motivos de tales restricciones.

Derecho de cancelación o eliminación

La letra h) del artículo 2° de la señalada ley, define la eliminación o cancelación de datos como "la destrucción de datos almacenados en registros o bancos de datos, cualquiera fuere el procedimiento empleado para ello". La cancelación corresponderá, y podrá ser solicitada por el titular, cuando su almacenamiento carezca de fundamento legal o cuando estuvieren caducos, debiendo, por tanto, quedar eliminados o destruidos de la base de datos.

Este derecho no es absoluto sino contingente y contextual, y requiere un equilibrio difícil de intereses y principios. El ejercicio del derecho plantea necesariamente cuestiones fundamentales en lo que se refiere no solo a la privacidad, el honor y la dignidad, sino también al derecho de acceso a la verdad, la libertad de información y de expresión, y la proporcionalidad.

Derecho de bloqueo

El Derecho a bloqueo consiste en la suspensión temporal de cualquier operación de tratamiento de los datos almacenados. Según el inciso tercero del artículo 6°; "Se bloquearán los datos personales cuya exactitud no pueda ser establecida o cuya vigencia sea dudosa y respecto de los cuales no corresponda la cancelación". El bloqueo incumbe a los responsables de bancos de datos personales. Este derecho se ejerce de manera subsidiaria a la eliminación, cuando el

derechos del interesado y se impidan entre otras cosas, efectos discriminatorios en las personas físicas por motivos de raza u origen étnico, opiniones políticas, religión o creencias, afiliación sindical, condición genérica o estado de salud u orientación sexual, o que den lugar a medidas que produzcan tal efecto".

titular revoque su consentimiento para el tratamiento de datos, o cuando el titular no quiera figurar en una base de datos de carácter comercial de forma temporal.

Otros derechos

Como se ha expuesto, los derechos de acceso, modificación, cancelación y bloqueo son los principales derechos establecidos en la legislación chilena, de igual forma es posible reconocer otros dos, contenidos también en la Ley N° 19.628. Como contrapartida al derecho a la información y acceso por parte de los titulares, la ley establece una obligación de comunicación a terceros por parte del responsable de datos personales. Esto se traduce en que, si se modifican o cancelan datos personales que han sido comunicados previamente a otras personas, el responsable del banco de datos deberá notificar de forma expedita acerca de la operación realizada, según lo dispone el inciso final del artículo 12. Es importante precisar la forma en que la norma plantea el derecho que nace para el titular de los datos a partir de la mencionada obligación, sin calificarlo expresamente como un derecho propiamente tal.

También el inciso final del artículo 3°establece el derecho de oposición: "El titular puede oponerse a la utilización de sus datos personales con fines de publicidad, investigación de mercado o encuestas de opinión".

El titular tiene el derecho de oponerse, debido a su situación particular, en cualquier momento, al tratamiento de sus datos personales cuando tenga una razón legítima para ello o cuando el tratamiento de información que le es propia tenga por objeto la mercadotecnia directa, incluida la elaboración de perfiles, en la medida que esté relacionada con dicha actividad. Cuando el titular se oponga al tratamiento con fines de mercadotecnia directa, sus datos personales deberían dejar de ser tratados para dichos fines.

El derecho de oposición es un derecho más de los cuales es titular el interesado y se relaciona con la licitud del tratamiento y con la autodeterminación informativa, propia del derecho a la protección de datos. A este derecho también hace referencia el considerando 70 del RGPD, al señalar: "si los datos personales son tratados con fines de mercadotecnia directa, el interesado debe tener derecho a oponerse a dicho tratamiento, inclusive a la elaboración de perfiles en la medida en que esté relacionada con dicha mercadotecnia, ya sea con respecto a un tratamiento inicial o ulterior, y ello en cualquier momento y sin coste alguno. Dicho derecho debe comunicarse explícitamente al interesado y presentar claramente y al margen de cualquier otra información".

Finalmente, el inciso primero del artículo 21 dispone: "Los organismos públicos que sometan a tratamiento datos personales relativos a condenas por delitos, infracciones administrativas o faltas disciplinarias, no podrán comunicarlos una vez prescrita la acción penal o administrativa, o cumplida o prescrita la sanción o la pena".

Esta disposición establece entonces, una especie de derecho al olvido, favorable para las personas que han sido infraccionadas con sanciones de tipo penal o administrativas, promoviendo la reinserción de las personas, salvo que los tribunales de justicia u otros servicios públicos en el ejercicio de las funciones que les son asignadas por ley soliciten esa información.

Sobre este punto, y como se ha dicho, si bien nuestra actual legislación no ha abordado el derecho al olvido, a diferencia del RGPD y la normativa española, existe un creciente abordaje doctrinario sobre el mismo, Gomes de Andrade señala "solo olvidando las identidades pasadas

podemos hacer que prevalezca la identidad real, el derecho a ser olvidado puede desarrollar un papel muy importante para que una persona pueda reconstruir su narrativa identitaria"[168].

Esta categorización de derechos derivados de la protección de datos, reconocida en el RGPD e incluidos en la Ley Orgánica de Protección de Datos y Garantías de Derechos Digitales - LOPDGDD de España, con la inclusión de los denominados derecho al olvido, derecho a la portabilidad[169] y derecho a la limitación en el tratamiento de datos, es lo que algunos han denominado los derechos ARCO PLUS.

El Reconocimiento constitucional del Derecho a la Protección de Datos en Chile

Desde los orígenes del ordenamiento constitucional chileno, es posible advertir el interés por el resguardo a la intimidad y vida privada, y de eso da cuenta la historia constitucional chilena fundamentalmente en las Cartas Políticas de 1833 y 1925, sin embargo no es sino, como señala Sanz Salguero, hasta el Acta Constitucional N° 3 del 11 de septiembre de 1976 (primera regulación en consagrar la protección de la vida privada de las personas en el ordenamiento constitucional chileno), antecedente directo e inmediato, que la Constitución Política de 1980 hace respecto a la tutela de este derecho[170], el que tiene su aterrizaje legislativo el año 1999 con la dictación de la Ley N° 19.628 sobre protección a la vida privada y que, como se verá, en el año 2018 consagra y reconoce a través de una reforma constitucional, a la protección de datos personales como un derecho fundamental.

La incorporación de la protección de datos personales a la Carta de 1980, además de las fuentes comparadas y doctrinarias ya señaladas en la presente investigación, tuvo como antecedente la jurisprudencia del Tribunal Constitucional (TC) chileno. En efecto, el TC en diversas sentencias dispuso en lo pertinente que "la protección a la vida privada de las personas guarda una estrecha relación con la protección de los datos personales, configurando lo que la doctrina llama derecho a la autodeterminación informativa." "Ello se traduce en el control de las

[168] Gomes de Andrade, N. (2012), "El olvido: el derecho a ser diferente de uno mismo. Una reconsideración del derecho a ser olvidado", IDP, *Revista de Internet, Derecho y Política*, n° 13, p.4.

[169] En Latinoamérica el alcance del derecho a la portabilidad de los datos personales es un tema emergente, que continúa siendo discutido al interior de algunos Estados, en particular respecto a los datos que abarca y si debe abordarse de manera general o sectorizada. Un número significativo de Estados Miembros de la OEA coinciden en que, cuando se procesen datos personales por vía electrónica o medios automatizados, el titular tendrá derecho a obtener una copia de los datos personales que hubiere proporcionado al Responsable en un formato electrónico estructurado, de uso común y lectura mecánica, que le permita seguir utilizándolos y transferirlos a otro Responsable sin impedimento, en caso de que lo requiera. El titular podrá solicitar que sus datos personales se transfieran directamente de Responsable a Responsable, cuando sea técnicamente posible. El derecho a la portabilidad de los datos no afectará negativamente los derechos y libertades de otros. Sin perjuicio de otros derechos del titular, el derecho a la portabilidad no debería resultar procedente cuando se trate de información inferida, derivada, creada, generada u obtenida a partir del análisis o tratamiento efectuado por el Responsable con base en los datos personales proporcionados por el titular, como es el caso de los datos personales que hubieren sido sometidos a un proceso de personalización, recomendación, categorización o creación de perfiles.

[170] Sanz Salguero, F. (2017), "Grado de Equivalencia entre la Protección de los Datos Personales y el Derecho de Acceso a la Información Pública", *Revista de Derecho de la Pontificia Universidad Católica de Valparaíso*, XLVIII, 1° semestre, pp.135-163.

personas sobre sus datos y comprende el derecho a saber sobre la existencia de ficheros o archivos de registros de información de carácter personal, público o privados, cuáles son sus finalidades y quiénes son los responsables de los mismos, de manera que las personas concernidas puedan conocer los datos propios contenidos en dichos archivos o ficheros, teniendo el derecho a actualizarlos o a solicitar mediante el recurso de habeas data su rectificación o cancelación"[171]. Como se puede observar, el Tribunal si bien distingue o reconoce el derecho a la protección de datos, lo vincula con el derecho al respeto y protección a la vida privada.

Solo en dos ocasiones desde la vigencia de la Constitución de 1980 se han incorporado nuevos derechos fundamentales[172], la primera vez en el numeral 25 del artículo 19 de la Carta, donde se reconoce la libertad de creación artística. Derecho que se incluye en el respectivo catálogo a través de la ley de reforma constitucional N° 19.742, publicada en el Diario Oficial el 25 de agosto del año 2001[173]que elimina la censura cinematográfica sustituyéndola por un sistema de calificación, consagrando además el derecho a la libre creación artística.

La segunda vez que se introduce un nuevo derecho fundamental de manera expresa en la Constitución chilena es en el año 2018, precisamente con el reconocimiento constitucional del derecho a la protección de datos personales. Antes de ese año la protección de datos se entendía contenida o subsumida en el derecho al respeto y protección a la vida privada.

El 11 de junio del año 2014 se inició la tramitación legislativa, vía moción parlamentaria[174], con la finalidad de introducir en el Capítulo III de la Constitución, "De las Garantías Constitucionales", en el numeral cuarto del artículo 19 a la protección de datos. El texto de la moción original era el siguiente:

"Artículo único: Modifíquese el artículo 19 N° 4 de la Constitución Política de la república, agregándose los siguientes incisos segundo y terceros nuevos:

Toda persona tiene derecho a la protección de sus datos personales y obtener su rectificación, complementación y cancelación, si éstos fueren erróneos o afectaren sus derechos, como asimismo a manifestar su oposición, de acuerdo con las disposiciones establecidas en la ley.

Su tratamiento sólo podrá hacerse por ley o con el consentimiento expreso del titular".

Como se puede apreciar, el legislador chileno en esta primera etapa no solo pretendió consagrar constitucionalmente el derecho a la protección de datos como derecho fundamental reconocido expresamente en la Carta, sino además regular su contenido estableciendo los denominados derechos ARCO (acceso, rectificación, cancelación y oposición).

---

[171] STC Roles números 1732-10 y 1800-10 de 21 de junio de 2011, considerando 25°.

[172] Conviene precisar eso sí que a través de otras reformas constitucionales se han introducido a los derechos fundamentales ya existentes otros atributos, solo a modo de ejemplo se puede señalar la Ley N° 19.876, que dispone la obligatoriedad y gratuidad de la educación media.

[173] Ver en: https://www.bcn.cl/leychile/navegar?idNorma=188827

[174] La tramitación legislativa en Chile puede iniciarse por dos vías, ya sea por moción parlamentaria, cuando la iniciativa es del Senado o la Cámara de Diputados, o por Mensaje Presidencial cuando la iniciativa la promueve el Ejecutivo (Presidente de la República), de ello da cuenta el inciso primero de la Constitución chilena: "Las leyes pueden tener su origen en la Cámara de Diputados o en el Senado, por mensaje que dirija el Presidente de la República o por moción de cualquiera de sus miembros. Las mociones no pueden ser firmadas por más de diez diputados ni por más de cinco senadores".

Más todavía, le imponía una limitación al legislador para la afectación del derecho de protección de datos, en términos en que esta solo podría hacerse por ley, lo que es coincidente con lo establecido en la Constitución chilena en el N° 26 del art.19, en orden a que las limitaciones a las garantías constitucionales solo pueden hacerse mediante preceptos legales, o en su defecto, por consentimiento expreso de su titular, impidiendo con ello el tratamiento de los datos que se alojan en fuentes de acceso público.

En efecto, el derecho a la protección de datos contempla como mínimo el respeto a los derechos ARCO y estos podrían ser considerados parte del núcleo esencial del mismo. Además, el mandato al legislador implica su reconocimiento explícito con el objeto de hacer posible su efectivo ejercicio.

Con el devenir del análisis y de la discusión legislativa, finalmente el texto que se plasmó en el N° 4 del artículo 19 fue el siguiente:

"El respeto y protección a la vida privada y a la honra de la persona y su familia y asimismo la protección de sus datos personales. El tratamiento y protección de estos datos se efectuará en la forma y condiciones que determine la ley".

De esta redacción se equipara la protección de datos personales a los tradicionales derechos de respeto y protección a la vida privada y a la honra personal y familiar, en el sentido de investirlo de la misma tutela o resguardo del que gozan dichos derechos fundamentales reconocidos constitucionalmente, mediante el denominado recurso de protección (una especie de *habeas corpus* referido en este caso no a la persona que se encuentra privada de libertad, sino a los datos de una persona), que se encuentra consagrado en el artículo 20 de la Constitución Política de Chile

Pero lo más importante, esta redacción constitucional a continuación de la expresión "asimismo", le reconoce a la protección de datos, tal como lo había hecho la doctrina y los ordenamientos jurídicos comparados, independencia y autonomía, dotándolo de un contenido y alcance propios. Reconociéndolo no solo en su dimensión negativa, para que no se utilicen esos datos sin el consentimiento de su titular, sino que, en su dimensión positiva, esto es el derecho a disponer de los mismos, consagrando así la libertad de los datos o la autodeterminación informativa.

A pesar de lo dicho, si se analiza el devenir legislativo desde la moción original, hasta la que finalmente se consagra en la ley aprobada por el Congreso chileno, no solo se excluyen los derechos ARCO de la redacción constitucional, sino que también la referencia al consentimiento expreso del titular para realizar el tratamiento de datos[175].

De igual forma sobre este punto, conviene tener a la vista la regulación que sobre el derecho a la protección de datos personales tienen importantes instrumentos jurídicos internacionales como la Carta de Derechos Fundamentales de la Unión Europea[176] y que podría haber sido de

[175] Durante la tramitación legislativa se hizo referencia a la experiencia comparada, en el sentido que no se empela la expresión consentimiento expreso o tácito, si no que la referencia se hace al consentimiento inequívoco, por lo que finalmente se recomendó y acogió eliminar la referencia al consentimiento, ya que es un concepto que ha variado en el tiempo.

[176] Artículo 8 Protección de datos de carácter personal 1. Toda persona tiene derecho a la protección de los datos de carácter personal que le conciernan. 2. Estos datos se tratarán de modo leal, para fines concretos y sobre la base del consentimiento de la persona afectada o en virtud de otro fundamento legítimo previsto por la ley. Toda

referencia para la regulación constitucional chilena. En efecto, de la disposición europea es posible distinguir los siguientes elementos para la configuración del derecho a la protección de datos personales:

1. Establece los principios de licitud, lealtad y finalidad;
2. Se reconocen los derechos de acceso y rectificación;
3. Se dispone de un mecanismo de garantía institucional reservado al establecimiento de una autoridad de control independiente[177].

Así, con fecha 16 de junio de 2018 se publicó en el Diario Oficial la ley N° 21.096, que consagra la protección de datos personales como garantía constitucional, en el numeral 4° del artículo 19 de la Constitución chilena[178].

Este significativo avance debe necesariamente ir acompañado con una nueva legislación que no solo de cuenta de la nueva era digital y tecnológica por la que estamos atravesando, sino que además reconozca y les dé un adecuado tratamiento a los denominados derechos ARCO, cuestión que la actual legislación chilena no hace. Y, todavía más importante, que estructure una entidad o autoridad de control encargada no solo de proteger y fiscalizar tanto a instituciones públicas como privadas en el cumplimiento efectivo del respeto a la protección de datos personales como derecho fundamental, sino además se encargue de su promoción y del desarrollo de acciones preventivas para su resguardo.

La Protección de Datos en la OCDE

Siguiendo en el ámbito europeo, en el año 2013, la OCDE actualiza sus directrices relacionadas con la protección de datos donde incorpora nuevos conceptos, tales como el principio de responsabilidad o rendición de cuentas, *"accountability"*, que en la práctica implica, entre otras cuestiones, que los responsables del tratamiento adopten programas de cumplimiento efectivo de la normativa sobre protección de datos personales. Se trata, por tanto, de que se establezcan "puertos seguros" en las organizaciones, que permitan gestionar el riesgo que supone y conlleva todo tratamiento de datos personales. Otro de los conceptos es el de notificación de las vulneraciones de seguridad, reforzando así el deber de seguridad

persona tiene derecho a acceder a los datos recogidos que le conciernan y a obtener su rectificación. 3. El respeto de estas normas estará sujeto al control de una autoridad independiente.

[177] La Constitución chilena ya ha establecido órganos de naturaleza independiente para resguardar un derecho fundamental especifico, como ocurre con el Consejo Nacional de Televisión, entidad autónoma que tutela en lo que le corresponde la libertad de opinión e información prevista en el art. 19 N° 12.

[178] "El que por causa de actos u omisiones arbitrarios o ilegales sufra privación, perturbación o amenaza en el legítimo ejercicio de los derechos y garantías establecidos en el artículo 19, números 1º, 2º, 3º inciso quinto, 4º, 5º, 6º, 9º inciso final, 11º,12º, 13º, 15º, 16º en lo relativo a la libertad de trabajo y al derecho a su libre elección y libre contratación, y a lo establecido en el inciso cuarto, 19º, 21º, 22º, 23º, 24°, y 25º podrá ocurrir por sí o por cualquiera a su nombre, a la Corte de Apelaciones respectiva, la que adoptará de inmediato las providencias que juzgue necesarias para restablecer el imperio del derecho y asegurar la debida protección del afectado, sin perjuicio de los demás derechos que pueda hacer valer ante la autoridad o los tribunales correspondientes. Procederá, también, el recurso de protección en el caso del Nº 8º del artículo 19, cuando el derecho a vivir en un medio ambiente libre de contaminación sea afectado por un acto u omisión ilegal imputable a una autoridad o persona determinada".

que es clave para garantizar la protección de datos personales.

El cumplimiento o *"enforcement"* es otro de los aspectos a los que presta atención la OCDE, siendo la primera vez que las directrices se refieren a las autoridades de protección de datos *"privacy enforcement authorities"*. Al respecto, la OCDE ha sido la impulsora de la Red Global de Autoridades de Protección de Datos, *"Global Privacy Enforcement Network"*, en la que participa por entre otras la Agencia Española de Protección de Datos.

En cuanto a las transferencias internacionales, las directrices se adaptan a la nueva realidad, la del *cloud computing*. La OCDE, en aras a facilitar el flujo internacional de los datos, alerta sobre la responsabilidad o *"accountability"* del responsable del tratamiento, con independencia de que este se encuentre en un modelo basado en el "nivel adecuado" de un país o en el uso de medidas tales como las normas corporativas vinculantes *Binding Corporate Rules, BCR* o las reglas de privacidad transfronterizas o *Cross-Border Privacy Rules, CBPRs*.

Por último, otra de las novedades relevantes es el impulso de políticas públicas de manera integral, en las que no se trata solo de adoptar medidas legislativas, sino de impulsar también una cultura en materia de protección de datos y privacidad.

La Actualización del Convenio 108

Estas directrices, que si bien tienen una importante influencia entre los países miembros de la OCDE[179] y para el resto del mundo, no son jurídicamente vinculantes para los Estados. Por lo que el Consejo de Europa adoptó el Convenio 108, instrumento internacional jurídicamente vinculante que tiene por objeto garantizar aquellos derechos vinculados a la intimidad, especialmente en lo que respecta al tratamiento de datos de carácter personal, consagrando internacionalmente el concepto de "protección de datos" como la protección o tutela jurídica de las personas con respecto al tratamiento automatizado de datos personales relativos al interesado.

Este Convenio es una norma jurídica internacional de la mayor importancia, fundamentalmente por dos razones; la primera, porque es el primer instrumento jurídico internacional que tiene fuerza obligatoria para los Estados, y en segundo lugar, es una pieza clave para la configuración de un nuevo derecho, que aunque relacionado con la intimidad y la protección a la vida privada tiene una configuración propia y autónoma, como es la protección de datos, conceptos constitucionalmente protegidos y reconocidos también en el artículo 8 del Convenio Europeo de Derechos Humanos CEDH, constituyéndose como el punto de partida para la cooperación internacional y la homogenización en materia de protección a la vida privada y el tratamiento automatizado de datos de carácter personal. Así se desprende de su preámbulo publicado en el BOE (Boletín Oficial del Estado) N° 274 del 15 de noviembre de 1985, que señala:

"… Considerando que es deseable ampliar la protección de los derechos y de las libertades fundamentales de cada uno, concretamente el derecho al respeto de la vida privada, teniendo

[179] Cabe señalar que la OCDE aglutina actualmente a 34 países miembros, siendo España uno de ellos. Por tanto, estas directrices son un referente, tanto en la Unión Europea como en otras latitudes alrededor del mundo que incluyen países tales como Israel, Japón Australia, Canadá, Chile, México o, incluso, Estados Unidos.

en cuenta la intensificación de la circulación a través de las fronteras de los datos de carácter personal que son objeto de tratamientos automatizados. Reafirmando al mismo tiempo su compromiso a favor de la libertad de información sin tener en cuenta las fronteras; Reconociendo la necesidad de conciliar los valores fundamentales de respeto a la vida privada y de la libre circulación de la información entre los pueblos…".

En el año 2010 se inició un proceso de actualización del Convenio 108, para alcanzar fundamentalmente los siguientes objetivos: dar cuenta de los nuevos desafíos derivados de la utilización de las tecnologías de la información y la comunicación, TIC, reforzar la aplicación del Convenio 108 junto con su mecanismo de seguimiento, y abordar la globalización de los flujos transfronterizos de datos personales.

La primera etapa de modernización fue encomendada al Comité Consultivo del Convenio 108 (T-PD), acordando las propuestas en su Vigésima Novena sesión plenaria realizada entre el 27 y 30 de noviembre de 2012. Esas propuestas fueron posteriormente examinadas en los años 2013 y 2014 por un Comité Intergubernamental Comité Ad Hoc sobre Protección de Datos - CAHDATA, que finalizó su trabajo en una última reunión celebrada los días 15 y 16 de junio de 2016[180].

La redacción de la propuesta estableció un consenso claro en que debía mantenerse el carácter general y tecnológicamente neutral de las disposiciones del Convenio 108, preservando la coherencia y la compatibilidad con otros marcos jurídicos relacionados.

Un gran desafío que la modernización del Convenio 108 debió asumir fue enfrentar los nuevos retos para la privacidad. Para ello, la modernización sigue, entre otras cosas, los parámetros establecidos en el documento elaborado por el Comité de la Convención 108, denominado *Guidelines on the protection of individuals with regard to the processing of personal data in a world of Big Data*, de 2017. Documento que tiene como objetivo principal hacer efectivos los principios y disposiciones del Convenio 108 en el contexto actual del *Big Data*. Estando dirigido a los controladores y procesadores de la información, para que puedan tener una guía a la hora de controlar y proteger los datos personales en este contexto tecnológico, hasta la definitiva aprobación del Convenio 108 en su versión actualizada[181].

Entre las modificaciones introducidas está la regulación de los denominados datos anónimos y su tutela. En principio, los datos anónimos no encajarían en la definición de datos personales ofrecida por el Convenio, porque no deberían permitir la identificación del individuo que ha entregado esos datos, ya que se entiende se han obtenido bajo anonimato, sin embargo, producto del avance de la tecnología, es posible identificar a los individuos a los que pertenecen esos datos anónimos, por lo que este riesgo de reidentificación adquiere una importancia considerable. Por lo anterior, la modernización del Convenio hace hincapié en este punto, ya que ahora, los datos anónimos entrarían dentro de la categoría de datos personales definidos por el Convenio 108.

---

[180] Ver: https://www.coe.int/es/web/data-protection/convention108/modernised Consultado el 17 de abril de 2020.

[181] Council of Europe, T-PD (2017)01, *Guidelines on the protection of individuals with regard to the processing of personal data in a world of Big Data, Strasbourg*, 2017, p.1. Disponible en https://rm.coe.int/16806ebe7a. Consultado el 17 de abril de 2020 108, pp. 3 y 7.

De igual manera, en esta actualización se alerta sobre los peligros que entraña el *Big data* considerando la infinidad de posibilidades que puede ofrecer el tratamiento de datos en masa y los riesgos que conlleva, debiendo incitar a los responsables del tratamiento de los datos a considerar la noción de control, ya no solo individualmente, sobre los datos que se estén tratando en un momento puntual, sino también de manera preventiva en cuanto al uso y al impacto en la dignidad humana que las técnicas del *Big data* pueden llegar a suponer.

La actualización o modernización del Convenio, también incluye nuevos datos dentro de la "especial categoría de datos", a los que se refiere el art. 6, que eran aquellos que gozaban de una mayor protección en el Convenio 108, ya que son datos más "sensibles" en el sentido de que se refieren a la zona más íntima de la personalidad. Así, se incluyen, por ejemplo, los datos biométricos o de ADN. Además, se amplía de alguna manera el catálogo de derechos, que incluye, por ejemplo, el derecho a saber por qué un computador tomó una decisión sobre cierta persona, como, por ejemplo, la no atribución de un beneficio social, o incluso si esa decisión fue tomada por una máquina altamente sofisticada[182].

Otra de las debilidades del convenio que han requerido actualizaciones es la que dice relación con los principios en él contenidos y su efectiva verificación por un órgano o instancia ajena a las partes que suscribieron el Convenio, en esa línea la modernización propuesta mejora las competencias del Comité Consultivo (T-PD) para permitir un mayor seguimiento y evaluación de la Convención en su aplicación por las partes. De esta forma, el Comité Consultivo o T-PD preparará, antes de cualquier nueva adhesión a la Convención, un dictamen para el Comité de Ministros sobre el nivel de protección de datos del candidato a adherir al Convenio examinando periódicamente la aplicación por las Partes, definiendo las medidas que deberán adoptarse cuando una de estas no esté conforme con la Convención.

Asimismo, facilitará, cuando sea necesario, la solución amistosa de todas las dificultades relacionadas con la aplicación del Convenio.

Esta modificación, impulsa también la cooperación y colaboración entre los Estados que la suscriban, al proponer que las Autoridades de Protección de Datos formen una red para el desempeño de sus funciones y se asistan mutuamente, otorgándoles más facultades e independencia, reduciendo las eventuales interferencias políticas en su quehacer.

Finalmente, el tercer aspecto abordado en la actualización del Convenio, es el de los flujos transfronterizos de datos personales, debido a su crecimiento globalizado se hace hincapié en el aspecto regulado en el Protocolo (Transferencias a Estados u Organizaciones Internacionales que no son parte de la Convención). Se busca garantizar que los datos personales tratados originalmente en la jurisdicción de una Parte (datos recopilados o almacenados, por ejemplo), que posteriormente estarán bajo la jurisdicción de un Estado que no es Parte de la Convención, continúen procesándose con las salvaguardias apropiadas.

Partiendo del principio de libre circulación o libre flujo entre Estados Parte, se distinguen las condiciones de transferencia a países que formen parte de uniones regionales (como la UE),

[182] Secretary General Speech, "*Convention 108: from a European reality to a global treaty: Modernising the Convention"*, 17 June 2016. Disponible en http://www.coe.int/en/web/secretary-general/-/-convention-108-from-a-european-reality-to-a-global-treaty-. Consultado el 20 de abril de 2020.

y a terceros países[183] u Organizaciones Internacionales, y cómo se deben evaluar las condiciones de "un nivel adecuado de protección" para realizar las transferencias. Además, se propone que las Autoridades de Protección tengan competencias en ciertos casos, pudiendo requerir al transferente que dé muestra de las garantías apropiadas, o incluso prohibir o suspender ciertas transferencias.

La Protección de Datos en el Tratado de la UE y en el Tratado de Funcionamiento de la Unión Europea

Siguiendo con el desarrollo europeo de la protección de datos de carácter personal desde una perspectiva normativa supra estatal, es necesario remitirse a dos instrumentos jurídicos internacionales de la mayor relevancia, el Tratado de la Unión Europea, TUE[184] y el Tratado de Funcionamiento de la Unión Europea, TFUE[185].

En efecto, el artículo 39 del TUE, dispone:

"De conformidad con el artículo 16 del Tratado de Funcionamiento de la Unión Europea, y no obstante lo dispuesto en su apartado 2, el Consejo adoptará una decisión que fije las normas sobre protección de las personas físicas respecto del tratamiento de datos de carácter personal por los Estados miembros en el ejercicio de las actividades comprendidas en el ámbito de aplicación del presente capítulo, y sobre la libre circulación de dichos datos. El respeto de dichas normas estará sometido al control de autoridades independientes".

A su vez el artículo 16 del TFUE, establece:

"Toda persona tiene derecho a la protección de los datos de carácter personal que le conciernan.

El Parlamento Europeo y el Consejo establecerán, con arreglo al procedimiento legislativo ordinario, las normas sobre protección de las personas físicas respecto del tratamiento de datos de carácter personal por las instituciones, órganos y organismos de la Unión, así como por los Estados miembros en el ejercicio de las actividades comprendidas en el ámbito de aplicación del Derecho de la Unión, y sobre la libre circulación de estos datos. El respeto de dichas normas estará sometido al control de autoridades independientes.

Las normas que se adopten en virtud del presente artículo se entenderán sin perjuicio de las normas específicas previstas en el artículo 39 del Tratado de la Unión Europea".

Como se puede advertir, estos tratados no solo reconocen el derecho a la protección de datos de carácter personal, sino que además facultan a la Unión Europea (UE) para regular y resguardar este derecho, lo que se traduce en que la UE y sus organismos, se encuentran habilitados para dictar reglamentos y directivas conducentes a tutelar la protección de datos.

---

[183] Sobre este punto hay que considerar que, a nivel latinoamericano, el Convenio ha sido suscrito por Uruguay primero el 10 de octubre de 2018 y luego por Argentina, el 19 de septiembre de 2019, los dos únicos países de los latinoamericanos en adherirse.

[184] Ver:http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2008:115:0013:0045:es:PDF.Revisión realizada el 20 de abril de 2020.

[185] Ver: https://www.boe.es/doue/2010/083/Z00047-00199.pdf. Revisión realizada el 20 de abril 2020.

De igual forma dichos preceptos hacen referencia a que serán autoridades de control independientes, esto es organismos o agencias especializadas con autonomía, las encargadas de resguardar la protección de datos.

Como se señalara anteriormente, otra pieza trascendental en el ámbito europeo para el desarrollo de la protección de datos es la Carta de Derechos Fundamentales de la Unión Europea, CDFUE[186], que como su nombre lo indica consagró por primera vez a nivel europeo un catálogo de derechos fundamentales[187].

Si bien en sus orígenes, en el año 2000, la Carta no fue vinculante, luego, con la entrada en vigor del Tratado de Lisboa en el año 2007 se convierte en un documento jurídicamente vinculante para los Estados miembros de la UE[188]. Y en lo que es objeto de este trabajo, como ya se señaló, consagra el derecho a la protección de datos de carácter personal en su artículo 8 como un derecho autónomo e independiente, llamativamente a continuación del derecho a

[186]Ver:http://www.derechoshumanos.net/normativa/normas/europa/CDFUE/CartaDerechosFundamentalesUnionEuropea-v2007.htm. Revisión realizada el 20 de abril 2020.

[187] Interesante es observar aquí la importancia del propósito de la CDFUE, al exponer en el preámbulo su declaración de intenciones: "Los pueblos de Europa, al crear entre sí una unión cada vez más estrecha, han decidido compartir un porvenir pacífico basado en valores comunes.

Consciente de su patrimonio espiritual y moral, la Unión está fundada sobre los valores indivisibles y universales de la dignidad humana, la libertad, la igualdad y la solidaridad, y se basa en los principios de la democracia y el Estado de Derecho. Al instituir la ciudadanía de la Unión y crear un espacio de libertad, seguridad y justicia, sitúa a la persona en el centro de su actuación.

La Unión contribuye a defender y fomentar estos valores comunes dentro del respeto de la diversidad de culturas y tradiciones de los pueblos de Europa, así como de la identidad nacional de los Estados miembros y de la organización de sus poderes públicos a escala nacional, regional y local; trata de fomentar un desarrollo equilibrado y sostenible y garantiza la libre circulación de personas, servicios, mercancías y capitales, así como la libertad de establecimiento.

Para ello es necesario, dándoles mayor proyección mediante una Carta, reforzar la protección de los derechos fundamentales a tenor de la evolución de la sociedad, del progreso social y de los avances científicos y tecnológicos.

La presente Carta reafirma, dentro del respeto de las competencias y misiones de la Unión, así como del principio de subsidiariedad, los derechos que emanan en particular de las tradiciones constitucionales y las obligaciones internacionales comunes a los Estados miembros, del Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales, las Cartas Sociales adoptadas por la Unión y por el Consejo de Europa, así como de la jurisprudencia del Tribunal de Justicia de la Unión Europea y del Tribunal Europeo de Derechos Humanos. En este contexto, los órganos jurisdiccionales de la Unión y de los Estados miembros interpretarán la Carta atendiendo debidamente a las explicaciones elaboradas bajo la autoridad del Praesidium de la Convención que redactó la Carta y actualizadas bajo la responsabilidad del Praesidium de la Convención Europea.

El disfrute de tales derechos conlleva responsabilidades y deberes tanto respecto de los demás como de la comunidad humana y de las generaciones futuras.

En consecuencia, la Unión reconoce los derechos, libertades y principios enunciados a continuación".

[188] En el caso de España, debe tenerse en cuenta que con anterioridad a la entrada en vigor del Tratado de Lisboa, el artículo 2 de la Ley Orgánica 1/2008, de 30 de julio, ya establecía lo siguiente: "A tenor de lo dispuesto en el párrafo segundo del artículo 10 de la Constitución española y en el apartado 8 del artículo 1 del Tratado de Lisboa, las normas relativas a los derechos fundamentales y a las libertades que la Constitución reconoce se interpretarán también de conformidad con lo dispuesto en la Carta de los Derechos Fundamentales publicada en el *Diario Oficial de la Unión Europea* de 14 de diciembre de 2007".

la protección a la vida privada y familiar, lo que demuestra su independencia, pero también su intrínseca relación. El artículo 8 de la CDFUE establece:

"Toda persona tiene derecho a la protección de los datos de carácter personal que la conciernan. Estos datos se tratarán de modo leal, para fines concretos y sobre la base del consentimiento de la persona afectada o en virtud de otro fundamento legítimo previsto por la ley. Toda persona tiene derecho a acceder a los datos recogidos que la conciernan y a obtener su rectificación.
El respeto de estas normas estará sujeto al control de una autoridad independiente".

Como es posible advertir, la Carta no solo hace referencia expresa a la protección de datos personales como derecho fundamental, sino que también aporta en dos aspectos sustanciales; primero menciona los principios en materia de protección de datos, tales como el de finalidad, consentimiento, licitud y rectificación. Y en segundo lugar sujeta el cumplimiento de estas normas y principios a una autoridad de control independiente.

Con antelación a la Carta de Derechos Fundamentales de la Unión Europea, el principal instrumento jurídico sobre protección de datos a nivel europeo fue la Directiva 95/46CE del Parlamento Europeo y del Consejo de Europa de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos[189].

Hay autores[190] que han calificado esta Directiva, cuestión que se comparte, como un hito en la historia de la protección de datos personales en la Unión Europea, siendo el primer instrumento jurídico que reconoció a la protección de datos con independencia del derecho a la intimidad o la protección a la vida privada (recordar que la CDFUE y sus posteriores modificaciones a través del Tratado de Lisboa son posteriores a esta Directiva). Otros[191], consideran que esta Directiva no establece de manera explícita a la protección de datos de carácter personal como un derecho propiamente tal, ya que esta se focaliza, según se desprende de su propio título, en la protección de las personas físicas en lo que respecta al tratamiento de datos personales y la libre circulación de estos datos. No se comparte esta perspectiva, ya que no solo de los preámbulos, sino que, en su artículo primero, se refiere a la protección de los derechos fundamentales.

La importancia de la Directiva de la protección de datos es evidente, ya que no solo reguló por primera vez en el ámbito europeo esta materia, sino que entregó contenido y amplió los principios meramente declarativos del Convenio 108 del Consejo de Europa, introduciendo

[189]Ver: https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:31995L0046&from=EN consulta realizada el 20 de abril de 2020.

[190] Rallo Lombarte, A. (2012) "Hacia un nuevo sistema europeo de protección de datos: las claves de la reforma", *Revista de Derecho Político (UNRD)*, n° 85 (septiembre-diciembre), pp.17 y ss.

[191] González Fuster, G. (2015), "The Emergence of Personal Data Protection as a Fundamental Right of the EU", Bruselas, Springer.

además la figura de un supervisor independiente como entidad reguladora para el cumplimiento de la protección de datos.

En este sentido, ya el artículo 1 de la Directiva 95/46/CE establece sus objetivos al señalar:

"1. Los Estados miembros garantizarán, con arreglo a las disposiciones de la presente Directiva, la protección de las libertades y de los derechos fundamentales de las personas físicas, y, en particular, del derecho a la intimidad, en lo que respecta al tratamiento de los datos personales.
2. Los Estados miembros no podrán restringir ni prohibir la libre circulación de datos personales entre los Estados miembros por motivos relacionados con la protección garantizada en virtud del apartado 1".

En efecto, la norma busca equiparar la protección o tutela de los derechos y libertades de las personas, haciendo referencia al tratamiento de datos personales en todos los Estados miembros de la UE y facilitar la libre circulación de datos en el mercado interior. Estableciendo una obligación de los Estados miembros de garantizar todos los derechos fundamentales vinculados y no solo el derecho a la intimidad, absteniéndose de imponer restricciones a la libertad de circulación de los datos de carácter personal.

El artículo 2 de la Directiva se refiere a definiciones que conceptualizan términos tales como datos personales, tratamiento de datos personales y ficheros de datos personales, entre otros. La norma define los datos personales como; "toda información sobre una persona física identificada o identificable, el "interesado"; se considerará identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un número de identificación o uno o varios elementos específicos, característicos de su identidad física, fisiológica, psíquica, económica, cultural o social".

Por lo que se considera dato personal no solo aquellos datos pertenecientes a la esfera privada de la persona, sino que todo contenido o información que haga identificable a un individuo, como por ejemplo nombre, domicilio o actividad profesional.

Un aporte fundamental de esta normativa es que avanzó en uniformar la regulación y protección de datos personales entre todos los Estados miembros de la UE, al consagrar en su preámbulo y disposiciones una serie de principios, que, si bien algunos de ellos ya estaban enunciados en el Convenios 108, la Directiva los amplia y desarrolla, tal como da cuenta el considerando 11 de su preámbulo, que señala:

"Considerando que los principios de la protección de los derechos y libertades de las personas y, en particular, del respeto de la intimidad, contenidos en la presente Directiva, precisan y amplían los del Convenio de 28 de enero de 1981 del Consejo de Europa para la protección de las personas en lo que respecta al tratamiento automatizado de los datos personales"

Y a su vez los artículos 6 y 7 de la Directiva, establecen los principios relativos a la calidad de los datos y los principios relativos a la legitimación del tratamiento de datos respectivamente:

"Artículo 6:
1. Los Estados miembros dispondrán que los datos personales sean:
a) tratados de manera leal y lícita;
b) recogidos con fines determinados, explícitos y legítimos, y no sean tratados posteriormente de manera incompatible con dichos fines; no se considerará incompatible el tratamiento posterior de datos con fines históricos, estadísticos o científicos, siempre y cuando los Estados miembros establezcan las garantías oportunas;
c) adecuados, pertinentes y no excesivos con relación a los fines para los que se recaben y para los que se traten posteriormente;
d) exactos y, cuando sea necesario, actualizados; deberán tomarse todas las medidas razonables para que los datos inexactos o incompletos, con respecto a los fines para los que fueron recogidos o para los que fueron tratados posteriormente, sean suprimidos o rectificados;
e) conservados en una forma que permita la identificación de los interesados durante un período no superior al necesario para los fines para los que fueron recogidos o para los que se traten ulteriormente. Los Estados miembros establecerán las garantías apropiadas para los datos personales archivados por un período más largo del mencionado, con fines históricos, estadísticos o científicos…"

"Artículo 7°:
Los Estados miembros dispondrán que el tratamiento de datos personales sólo pueda efectuarse si:
a) el interesado ha dado su consentimiento de forma inequívoca, o
b) es necesario para la ejecución de un contrato en el que el interesado sea parte o para la aplicación de medidas precontractuales adoptadas a petición del interesado, o
c) es necesario para el cumplimiento de una obligación jurídica a la que esté sujeto el responsable del tratamiento, o
d) es necesario para proteger el interés vital del interesado, o
e) es necesario para el cumplimiento de una misión de interés público o inherente al ejercicio del poder público conferido al responsable del tratamiento o a un tercero a quien se comuniquen los datos, o
f) es necesario para la satisfacción del interés legítimo perseguido por el responsable del tratamiento o por el tercero o terceros a los que se comuniquen los datos, siempre que no prevalezca el interés o los derechos y libertades fundamentales del interesado que requieran protección con arreglo al apartado 1 del artículo 1 de la presente Directiva".

Los principios del artículo 6 de la Directiva han sido denominados por la doctrina[192] Principio de la Lealtad; Principio de Finalidad; Principio de utilización no abusiva; Principio de Pertinencia; Principio de Exactitud y Principio de Derecho al Olvido[193].

[192] Bru Cuadrada, E. (2007), "La protección de datos en España y en la Unión Europea. Especial referencia a los mecanismos jurídicos de reacción frente a la vulnerabilidad del derecho a la intimidad", *Revista de los Estudios de Derecho y Ciencia Política (IDP)*, n°5, pp.78-92.

[193] El Reglamento General de Protección de Datos (RGPD) 679/2016, agrega a estos principios en su artículo 12 el Principio de la Transparencia.

La Directiva también consagra otros principios como el Principio de Confidencialidad en su artículo 16[194], el Principio de Seguridad en su artículo 17[195] y el Principio de Acceso Individual, mediante los derechos de acceso y oposición previstos en los artículos 12[196] y 14[197] respectivamente.

---

[194] "Artículo 16: Confidencialidad del tratamiento

Las personas que actúen bajo la autoridad del responsable o del encargado del tratamiento, incluido este último, solo podrán tratar datos personales a los que tengan acceso, cuando se lo encargue el responsable del tratamiento o salvo en virtud de un imperativo legal".

[195] "Artículo 17: Seguridad del tratamiento

1. Los Estados miembros establecerán la obligación del responsable del tratamiento de aplicar las medidas técnicas y de organización adecuadas, para la protección de los datos personales contra la destrucción, accidental o ilícita, la pérdida accidental y contra la alteración, la difusión o el acceso no autorizados, en particular cuando el tratamiento incluya la transmisión de datos dentro de una red, y contra cualquier otro tratamiento ilícito de datos personales.

Dichas medidas deberán garantizar, habida cuenta de los conocimientos técnicos existentes y del coste de su aplicación, un nivel de seguridad apropiado en relación con los riesgos que presente el tratamiento y con la naturaleza de los datos que deban protegerse.

2. Los Estados miembros establecerán que el responsable del tratamiento, en caso de tratamiento por cuenta del mismo, deberá elegir un encargado del tratamiento que reúna garantías suficientes en relación con las medidas de seguridad técnica y de organización de los tratamientos que deban efectuarse, y se asegure de que se cumplen dichas medidas.

3. La realización de tratamientos por encargo deberá estar regulada por un contrato u otro acto jurídico que vincule al encargado del tratamiento con el responsable del tratamiento, y que disponga, en particular:

- que el encargado del tratamiento sólo actúa siguiendo instrucciones del responsable del tratamiento;

- que las obligaciones del apartado 1, tal como las define la legislación del Estado miembro en el que esté establecido el encargado, incumben también a éste.

4. A efectos de conservación de la prueba, las partes del contrato o del acto jurídico relativas a la protección de datos y a los requisitos relativos a las medidas a que hace referencia el apartado 1 constarán por escrito o en otra forma equivalente".

[196] Artículo 12: Derecho de acceso

Los Estados miembros garantizarán a todos los interesados el derecho de obtener del responsable del tratamiento:

a) libremente, sin restricciones y con una periodicidad razonable y sin retrasos ni gastos excesivos:

- la confirmación de la existencia o inexistencia del tratamiento de datos que le conciernen, así como información por lo menos de los fines de dichos tratamientos, las categorías de datos a que se refieran y los destinatarios o las categorías de destinatarios a quienes se comuniquen dichos datos;

- la comunicación, en forma inteligible, de los datos objeto de los tratamientos, así como toda la información disponible sobre el origen de los datos;

- el conocimiento de la lógica utilizada en los tratamientos automatizados de los datos referidos al interesado, al menos en los casos de las decisiones automatizadas a que se refiere el apartado 1 del artículo 15;

b) en su caso, la rectificación, la supresión o el bloqueo de los datos cuyo tratamiento no se ajuste a las disposiciones de la presente Directiva, en particular a causa del carácter incompleto o inexacto de los datos;

c) la notificación a los terceros a quienes se hayan comunicado los datos de toda rectificación, supresión o bloqueo efectuado de conformidad con la letra b), si no resulta imposible o supone un esfuerzo desproporcionado".

[197] "Artículo 14: Derecho de oposición del interesado

Los Estados miembros reconocerán al interesado el derecho a:

En su artículo 8 la Directiva estableció categorías especiales de tratamientos de datos, disponiendo en su apartado número 1 la prohibición general de tratar datos que dieran a conocer el origen racial o étnico, las opiniones políticas, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, así como el tratamiento de los datos relativos a la salud o a la sexualidad. Salvo, como se señala en el apartado 2 del mismo artículo 8, cuando el interesado haya dado su consentimiento explícito a dicho tratamiento, salvo en los casos en los que la legislación del Estado miembro disponga que la prohibición establecida en el apartado 1 no pueda levantarse con el consentimiento del interesado; o cuando el tratamiento sea necesario para respetar las obligaciones y derechos específicos del responsable del tratamiento en materia de Derecho laboral, en la medida en que esté autorizado por la legislación y ésta prevea garantías adecuadas; o cuando el tratamiento sea necesario para salvaguardar el interés vital del interesado o de otra persona, en el supuesto de que el interesado esté física o jurídicamente incapacitado para dar su consentimiento; o cuando el tratamiento sea efectuado en el curso de sus actividades legítimas y con las debidas garantías por una fundación, una asociación o cualquier otro organismo sin fin de lucro, cuya finalidad sea política, filosófica, religiosa o sindical, siempre que se refiera exclusivamente a sus miembros o a las personas que mantengan contactos regulares con la fundación, la asociación o el organismo por razón de su finalidad y con tal de que los datos no se comuniquen a terceros sin el consentimiento de los interesados; o, cuando el tratamiento se refiera a datos que el interesado haya hecho manifiestamente públicos o sea necesario para el reconocimiento, ejercicio o defensa de un derecho en un procedimiento judicial.

Antes de referirnos al Reglamento General de Protección de Datos RGPD, cuya vigencia data del año 2018, conviene hacer referencia a otras normas de alcance europeo que regularon la materia, ya sea porque no consideraban a los Estados miembros de la Unión o por que regulaban materias más específicas que la Directiva 95/46/CE. Tal como lo señala Martínez López- Sáez[198], la correlación es la siguiente:

- Directiva 97/66/EC Relativa al tratamiento de los datos personales y a la protección a la intimidad en el sector de las telecomunicaciones.
- Directiva 1001/58/CE Relativa al tratamiento de los datos personales y a la protección a la intimidad en el sector de las comunicaciones electrónicas.

---

a) oponerse, al menos en los casos contemplados en las letras e) y f) del artículo 7, en cualquier momento y por razones legítimas propias de su situación particular, a que los datos que le conciernan sean objeto de tratamiento, salvo cuando la legislación nacional disponga otra cosa. En caso de oposición justificada, el tratamiento que efectúe el responsable no podrá referirse ya a esos datos;

b) oponerse, previa petición y sin gastos, al tratamiento de los datos de carácter personal que le conciernan respecto de los cuales el responsable prevea un tratamiento destinado a la prospección; o ser informado antes de que los datos se comuniquen por primera vez a terceros o se usen en nombre de éstos a efectos de prospección, y a que se le ofrezca expresamente el derecho de oponerse, sin gastos, a dicha comunicación o utilización.

Los Estados miembros adoptarán todas las medidas necesarias para garantizar que los interesados conozcan la existencia del derecho a que se refiere el párrafo primero de la letra b)".

[198] Martínez López-Sáez, M. (2018), "Una revisión del derecho fundamental a la protección de datos de carácter personal", Tirante Lo Blanch, Valencia, p.77.

- Reglamento 45/2001 Relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones y los organismos comunitarios y la libre circulación de estos datos.
- Directiva 2006/24/EC Relativa a la conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones y por la que se modifica la Directiva 2002/58/CE (sobre conservación de datos, invalidada el 8 de abril de 2014).
- Directiva 2009/136/CE por la que se modifica la Directiva 2002/22/CE relativa al servicio universal y los derechos de los usuarios en relación con las redes y los servicios de comunicaciones electrónicas y la Directiva 2002/22/CE relativa al tratamiento de los datos personales y a la protección a la intimidad en el sector de las comunicaciones electrónicas y el Reglamento (CE) N°2006/2004 sobre cooperación en materia de protección de los consumidores.
- Decisión marco 2008/977/JAI Relativa a la protección de datos personales en el marco de la cooperación policial y judicial en materia penal.

El Reglamento General de Protección de Datos Personales RGPD

El Reglamento[199] de la Unión Europea 2016/679 del Parlamento Europeo y del Consejo de Europa del 27 de abril del 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, deroga la Directiva 95/46/CE y entra en vigor el 25 de mayo del año 2018 generando una importante alteración en la forma de operar de los responsables de las bases de datos personales. Este Reglamento es designado con el acrónimo RGPD.

Este nuevo régimen jurídico surge por cuanto se hacía indispensable reformular y actualizar la normativa jurídico internacional en materia de protección de datos. En efecto, la Directiva 95/46/CE surge en un contexto muy distinto al actual desarrollo que las tecnologías de la información y comunicación, además de la informática y las redes sociales han tenido en el actual siglo XXI. Por lo que esta nueva regulación además de introducir nuevos contenidos y alcances contribuye a consolidar el desarrollo del derecho a la protección de datos en el territorio de la Unión Europea mediante una norma única y de aplicación directa a todos los Estados miembros, con un doble propósito, coherencia en la aplicación normativa y evitar controversias que dificulten no solo la libre circulación, sino por sobre todo enerven la protección de los datos personales.

Objeto del RGPD

El RGPD se estructura en 173 considerandos, 11 capítulos y 99 artículos, su objeto está regulado en el artículo 1 y consiste en establecer las normas relativas a la protección de las personas físicas en lo que respecta al tratamiento de los datos personales y las normas relativas

[199] Ver: https://www.boe.es/doue/2016/119/L00001-00088.pdf. Revisión realizada el 21 de abril de 2020.

a la libre circulación de tales datos. Además de proteger los derechos y libertades fundamentales de las personas físicas y, en particular, su derecho a la protección de los datos personales.

Agrega que la libre circulación de los datos personales en la Unión no podrá ser restringida ni prohibida por motivos relacionados con la protección de las personas físicas en lo que respecta al tratamiento de datos personales.

Propósitos del RGPD

También de su considerando 2 es posible extraer los propósitos que el Reglamento persigue cuando señala que los principios y normas relativos a la protección de las personas físicas en lo que respecta al tratamiento de sus datos de carácter personal deben, con independencia de su nacionalidad o residencia, respetar sus libertades y derechos fundamentales, en particular el derecho a la protección de los datos de carácter personal. "El presente Reglamento pretende contribuir a la plena realización de un espacio de libertad, seguridad y justicia y de una unión económica, al progreso económico y social, al refuerzo y la convergencia de las economías dentro del mercado interior, así como al bienestar de las personas físicas".

También el reglamento tutela los derechos y libertades fundamentales de las personas físicas, que son los interesados[200] o beneficiarios de la protección de datos en la UE.

Ámbito de aplicación del RGPD

Sobre su ámbito de aplicación material y espacial se refieren los artículos 2 y 3 del Reglamento; en efecto, el artículo 3 sobre su aplicación territorial establece que se aplica al tratamiento de datos personales en el contexto de las actividades de un establecimiento del responsable o del encargado en la Unión, independientemente de que el tratamiento tenga lugar en la Unión o no; se aplica también al tratamiento de datos personales de interesados que residan en la Unión por parte de un responsable o encargado no establecido en la Unión, cuando las actividades de tratamiento estén relacionadas con: la oferta de bienes o servicios a dichos interesados en la Unión, independientemente si a estos se les requiere su pago o el control de su comportamiento, en la medida en que este tenga lugar en la Unión.

Además, este Reglamento se aplica al tratamiento de datos personales por parte de un responsable que no esté establecido en la Unión sino en un lugar en que el derecho de los Estados miembros se aplique en virtud del derecho internacional público.

Como se puede apreciar el Reglamento amplía entonces, bajo determinados supuestos, su aplicación territorial incluso fuera de la Unión Europea, lo que representa un avance con respecto a la Directiva 95/46/CE, por cuanto facilita el sometimiento a la normativa europea, y por consiguiente a sus tribunales (que incluye por cierto a los tribunales españoles) y en

[200] El RGPD en los considerandos 23 y 72 emplea la expresión interesados para referirse a las personas físicas.

última instancia al Tribunal de Justicia de la Unión Europea TJUE, de quienes aunque no se encuentren en la UE, transgredan las disposiciones del RGPD.

Nuevos términos definidos por el RGPD

Luego, en el artículo 4 el RGPD define nuevos términos, tales como datos genéticos, que son "datos personales relativos a las características genéticas heredadas o adquiridas de una persona física que proporcionen una información única sobre la fisiología o la salud de esa persona, obtenidos en particular del análisis de una muestra biológica de tal persona"; datos biométricos, que son "datos personales obtenidos a partir de un tratamiento técnico específico, relativos a las características físicas, fisiológicas o conductuales de una persona física que permitan o confirmen la identificación única de dicha persona, como imágenes faciales o datos dactiloscópicos"; los datos relativos a la salud, que son "datos personales relativos a la salud física o mental de una persona física, incluida la prestación de servicios de atención sanitaria, que revelen información sobre su estado de salud"; se refiere también a grupo empresarial, que es un "grupo constituido por una empresa que ejerce el control y sus empresas controladas"; define también las normas corporativas vinculantes como "las políticas de protección de datos personales asumidas por un responsable o encargado del tratamiento establecido en el territorio de un Estado miembro para transferencias o un conjunto de transferencias de datos personales a un responsable o encargado en uno o más países terceros, dentro de un grupo empresarial o una unión de empresas dedicadas a una actividad económica conjunta".

La Autoridad de Control en el RGPD

A su turno, el artículo 51 del Reglamento en su apartado 1 dispone que "Cada Estado miembro establecerá que sea responsabilidad de una o varias autoridades públicas independientes (en adelante "autoridad de control") supervisar la aplicación del presente Reglamento, con el fin de proteger los derechos y las libertades fundamentales de las personas físicas en lo que respecta al tratamiento y de facilitar la libre circulación de datos personales en la Unión" y luego agrega en el apartado 3 del mismo artículo: "Cuando haya varias autoridades de control en un Estado miembro, este designará la autoridad de control que representará a dichas autoridades en el Comité, y establecerá el mecanismo que garantice el cumplimiento por las demás autoridades de las normas relativas al mecanismo de coherencia a que se refiere el artículo 63[201]".

En el mismo sentido y considerando el ámbito europeo que se analiza, es importante destacar que el RGPD, en su artículo 68 crea el Comité Europeo de Protección de Datos como organismo de la Unión, que gozará de personalidad jurídica, y estará compuesto por el director de una autoridad de control de cada Estado miembro y por el Supervisor Europeo de Protección de Datos o sus representantes respectivos. Su regulación considera también que cuando en un

[201] "Artículo 63: Mecanismo de coherencia; A fin de contribuir a la aplicación coherente del presente Reglamento en toda la Unión, las autoridades de control cooperarán entre sí y, en su caso, con la Comisión, en el marco del mecanismo de coherencia establecido en la presente sección".

Estado miembro existan varias autoridades de control para la protección de datos, se nombrará a un representante común de conformidad con el Derecho de ese Estado miembro.

El Consentimiento del titular de los datos en el RGPD

También en el artículo 4 del Reglamento, en su apartado 11 se amplía la definición de consentimiento del interesado en relación con la anterior Directiva, al explicarlo como: "toda manifestación de voluntad libre, específica, informada e inequívoca por la que el interesado acepta, ya sea mediante una declaración o una clara acción afirmativa, el tratamiento de datos personales que le conciernen". Por consiguiente, para entender que el consentimiento es inequívoco debe existir una declaración de los interesados o una acción positiva que indique el acuerdo del interesado, agregando que el consentimiento debe ser explicito para autorizar el tratamiento de datos sensibles.

Por lo anterior, según lo dispone el Reglamento, no pueden existir consentimientos implícitos o presuntos, deben ser expresos, estos deben manifestarse en términos explícitos e inequívocos. Y, además, la carga de la prueba del consentimiento del interesado recae en el controlador que procesa los datos personales con determinados fines, pudiendo estos interesados en cualquier momento retirar su consentimiento.

Contenido y Alcance del tratamiento en el RGPD

El RGPD, al igual que la Directiva, prohíbe el tratamiento de datos que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, así como datos relativos a la salud, a la sexualidad o a las orientaciones sexuales de una persona física, y a su vez incorpora el tratamiento de datos genéticos, datos biométricos dirigidos, destinados a identificar de manera univoca a una persona física[202]. Lo que amplía entonces el tratamiento de datos relacionados con condenas penales y medidas de seguridad relacionadas con estas.

En cuanto al tratamiento de los datos de salud, el Reglamento configura una protección adicional, por cuanto se permite el procesamiento de esa información de salud siempre que la legislación europea o nacional disponga de garantías adecuadas para proteger los intereses de los titulares de dichos datos, y siempre y cuando estos datos sean necesarios para aspectos vinculados a la medicina preventiva o laboral, a la evaluación de la capacidad laboral del trabajador, al diagnóstico médico, a la prestación de asistencia o tratamiento de tipo sanitario o social, o a la gestión de los sistemas y servicios de asistencia sanitaria y social, sustentándose en el Derecho de la Unión o de los Estados miembros o de un contrato con un profesional sanitario, por razones de interés público en el ámbito de la salud pública o en áreas tales como

[202] Ver, apartado 1 del artículo 9, sobre Tratamiento de categorías especiales de datos personales; "Quedan prohibidos el tratamiento de datos personales que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, y el tratamiento de datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud o datos relativos a la vida sexual o las orientación sexuales de una persona física".

la protección social y por razones históricas, estadísticas, científicas o de investigación, en el entendido que tales efectos, no son posibles de alcanzarse de otro modo[203].

El Tratamiento de datos de niñas y niños en el RGPD

Otro aspecto novedoso introducido por el RGPD es la tutela específica para el tratamiento de datos personales de los niños menores de 16 años (el Reglamento permite que los Estados miembros puedan establecer por ley una edad inferior, siempre que esta no sea menor a los 13 años), estableciendo el requisito de que el consentimiento sea dado por los padres o el tutor legal en el caso de servicios de la sociedad de la información. Todo lo cual no afectará las normas contractuales de los derechos nacionales, ni tampoco las disposiciones relativas a la validez, formación o efectos de los contratos celebrados o suscritos con menores.

El Derecho de Rectificación en el RGPD

Desde la perspectiva de la protección de datos de carácter personal, como derecho fundamental, el Reglamento también avanza consagrando expresamente el derecho de rectificación, establecido en el artículo 16, que dispone;

"El interesado tendrá derecho a obtener sin dilación indebida del responsable del tratamiento la rectificación de los datos personales inexactos que le conciernan. Teniendo en cuenta los fines del tratamiento, el interesado tendrá derecho a que se completen los datos personales que sean incompletos, inclusive mediante una declaración adicional".

Por lo tanto, el interesado tendrá, por un lado, derecho a obtener sin dilación indebida del responsable del tratamiento la rectificación de los datos personales inexactos que le conciernan, y por otro, considerando los fines del tratamiento, la posibilidad de completar los datos personales incompletos, incluso con información adicional.

[203] Letras h); i) y j) del apartado 2 del artículo 9 del RGPD; Letra "h) el tratamiento es necesario para fines de medicina preventiva o laboral, evaluación de la capacidad laboral del trabajador, diagnóstico médico, prestación de asistencia o tratamiento de tipo sanitario o social, o gestión de los sistemas y servicios de asistencia sanitaria y social, sobre la base del Derecho de la Unión o de los Estados miembros o en virtud de un contrato con un profesional sanitario y sin perjuicio de las condiciones y garantías contempladas en el apartado 3"; Letra i) el tratamiento es necesario por razones de interés público en el ámbito de la salud pública, como la protección frente a amenazas transfronterizas graves para la salud, o para garantizar elevados niveles de calidad y de seguridad de la asistencia sanitaria y de los medicamentos o productos sanitarios, sobre la base del Derecho de la Unión o de los Estados miembros que establezca medidas adecuadas y específicas para proteger los derechos y libertades del interesado, en particular el secreto profesional; Letra "j) el tratamiento es necesario con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, de conformidad con el artículo 89, apartado 1, sobre la base del Derecho de la Unión o de los Estados miembros, que debe ser proporcional al objetivo perseguido, respetar en lo esencial el derecho a la protección de datos y establecer medidas adecuadas y específicas para proteger los intereses y derechos fundamentales del interesado".

También se refiere a este derecho el considerando 65 del Reglamento que en su primera línea dispone que: "Los interesados deben tener derecho a que se rectifiquen los datos personales que le conciernen…"

Como es posible advertir el derecho de rectificación se relaciona con el principio de exactitud, previsto en el artículo 5, punto 1, letra d), que establece a propósito de los principios relativos al tratamiento de los datos personales, señalando que estos deben ser exactos y, si fuera necesario, actualizados, debiendo adoptar todas las medidas razonables para que se supriman o rectifiquen sin dilación los datos personales que sean inexactos con respecto a los fines para los que se tratan.

Como señala Aparicio Salom, este derecho de rectificación que materializa el principio de exactitud, legitima al interesado a exigir del responsable del tratamiento que éste sea el fiel reflejo de la realidad, actualizando los datos cuando estos resulten inexactos o incompletos[204].

En otras palabras, el derecho de rectificación solo podrá ejercerse cuando los datos afectos a tratamiento sean inexactos, debiendo el responsable de los datos comprobar dentro de plazo la inexactitud denunciada, pudiendo para ello requerir al interesado para que especifique los datos que quiere rectificar.

El Derecho al Olvido

El derecho al olvido, también denominado derecho a la supresión de datos -aunque podríamos apreciar alguna diferencia entre ambos-, si bien no ha tenido un desarrollo uniforme en los ordenamientos jurídicos latinoamericanos ni tampoco en Chile, ha tenido un rápido y creciente progreso en el ámbito jurídico europeo. Como punto de partida nos hemos de referir a la sentencia del Tribunal de Justicia de la Unión Europea (TJUE) del 13 de mayo del 2014, caso Mario Costeja González y Agencia Española de Protección de Datos (AEPD) versus Google Spain y Google Inc., En el asunto prejudicial C-131/12, donde se le da al derecho al olvido un sentido y alcance mayor en un entorno virtual como es la obligación de supresión para todo responsable del tratamiento de datos en determinadas circunstancias en el contexto de motores de búsqueda en internet.

El caso Costeja v. Google

Los hechos, siguiendo lo dispuesto en los numerales 14 al 19 de la Sentencia fueron los siguientes: "El 5 de marzo de 2010, el Sr. Costeja González, de nacionalidad española y domiciliado en España, presentó ante la AEPD una reclamación contra La Vanguardia Ediciones, S.L., que publica un periódico de gran difusión, concretamente en Cataluña (en lo sucesivo, "La Vanguardia"), y contra Google Spain y Google Inc. Esta reclamación se basaba

[204] Aparicio Salom, J. (2018), "*Derechos del interesado (artículos 12-19), el nuevo marco regulatorio derivado del Reglamento Europeo de Protección de Datos"*. Adaptado al Proyecto de Ley Orgánica de Protección de Datos de 10 de noviembre de 2017, coordinador José López Calvo, Boch, Barcelona.

en que, cuando un internauta introducía el nombre del Sr. Costeja González en el motor de búsqueda de Google (en lo sucesivo, "Google Search"), obtenía como resultado vínculos hacia dos páginas del periódico La Vanguardia, del 19 de enero y del 9 de marzo de 1998, respectivamente, en las que figuraba un anuncio de una subasta de inmuebles relacionada con un embargo por deudas a la Seguridad Social, que mencionaba el nombre del Sr. Costeja González.

Mediante esta reclamación, el Sr. Costeja González solicitaba, por un lado, que se exigiese a La Vanguardia eliminar o modificar la publicación para que no apareciesen sus datos personales, o utilizar las herramientas facilitadas por los motores de búsqueda para proteger estos datos. Por otro lado, solicitaba que se exigiese a Google Spain o a Google Inc. que eliminaran u ocultaran sus datos personales para que dejaran de incluirse en sus resultados de búsqueda y dejaran de estar ligados a los enlaces de La Vanguardia. En este marco, el Sr. Costeja González afirmaba que el embargo al que se vio sometido estaba totalmente solucionado y resuelto desde hace años y carecía de relevancia actualmente.

Mediante resolución de 30 de julio de 2010, la AEPD desestimó la reclamación en la medida en que se refería a La Vanguardia, al considerar que la publicación que esta había llevado a cabo estaba legalmente justificada, dado que había tenido lugar por orden del Ministerio de Trabajo y Asuntos Sociales y, tenía por objeto dar la máxima publicidad a la subasta para conseguir la mayor concurrencia de licitadores. En cambio, se estimó la misma reclamación en la medida en que se dirigía contra Google Spain y Google Inc. A este respecto, la AEPD consideró que quienes gestionan motores de búsqueda están sometidos a la normativa en materia de protección de datos, dado que llevan a cabo un tratamiento de datos del que son responsables y actúan como intermediarios de la sociedad de la información. La AEPD consideró que estaba facultada para ordenar la retirada e imposibilitar el acceso a determinados datos por parte de los gestores de motores de búsqueda cuando considere que su localización y difusión puede lesionar el derecho fundamental a la protección de datos y a la dignidad de la persona entendida en un sentido amplio, lo que incluye la mera voluntad del particular afectado cuando quiere que tales datos no sean conocidos por terceros. La AEPD estimó que este requerimiento puede dirigirse directamente a los explotadores de motores de búsqueda, sin suprimir los datos o la información de la página donde inicialmente está alojada e, incluso, cuando el mantenimiento de esta información en dicha página esté justificado por una norma legal.

Google Spain y Google Inc. interpusieron sendos recursos contra dicha resolución ante la Audiencia Nacional, que decidió acumularlos. El mencionado tribunal expone en el auto de remisión que estos recursos plantean la cuestión de cuáles son las obligaciones que tienen los gestores de motores de búsqueda en la protección de datos personales de aquellos interesados que no desean que determinada información, publicada en páginas web de terceros, que contiene sus datos personales y permite relacionarles con la misma, sea localizada, indexada y sea puesta a disposición de los internautas de forma indefinida. Considera que la respuesta a esta cuestión depende del modo en que debe interpretarse la Directiva 95/46/CE en el marco de estas tecnologías, que han surgido después de su publicación.

Resolviendo en definitiva el TJUE que Google Spain y Google Inc. como gestores de los motores de búsqueda de la información que afecta al titular de los datos, en la especie el señor Costeja González ya no se ponga a disposición del público en general mediante su inclusión en una lista de resultados, ya que su derecho al olvido prevalece, en principio, no solo sobre el

interés económico del gestor del motor de búsqueda, sino también sobre el interés del público en acceder a la mencionada información en una búsqueda que verse sobre el nombre de esa persona.

El tiempo y la transcendencia pública de la información se van a convertir en los elementos sobre los que gravite la aplicación del derecho al olvido por parte de la propia entidad que trata los datos personales[205].

[205] Según el N° 2 de la Sentencia del TJUE, "Esta petición se presentó en el marco de un litigio entre Google Spain, S.L. (en lo sucesivo, "Google Spain"), y Google Inc., por un lado, y la Agencia Española de Protección de Datos (en lo sucesivo, "AEPD") y el Sr. Costeja González por otro, en relación con una resolución de dicha Agencia por la que se estimó la reclamación del Sr. Costeja González contra ambas sociedades y se ordenaba a Google Inc. que adoptara las medidas necesarias para retirar los datos personales del Sr. Costeja González de su índice e imposibilitara el acceso futuro a los mismos". Sentencia que además en su parte resolutiva resolvió: "1) El artículo 2, letras b) y d), de la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, debe interpretarse en el sentido de que, por un lado, la actividad de un motor de búsqueda, que consiste en hallar información publicada o puesta en Internet por terceros, indexarla de manera automática, almacenarla temporalmente y, por último, ponerla a disposición de los internautas según un orden de preferencia determinado, debe calificarse de "tratamiento de datos personales", en el sentido de dicho artículo 2, letra b), cuando esa información contiene datos personales, y, por otro, el gestor de un motor de búsqueda debe considerarse "responsable" de dicho tratamiento, en el sentido del mencionado artículo 2, letra d). 2) El artículo 4, apartado 1, letra a), de la Directiva 95/46 debe interpretarse en el sentido de que se lleva a cabo un tratamiento de datos personales en el marco de las actividades de un establecimiento del responsable de dicho tratamiento en territorio de un Estado miembro, en el sentido de dicha disposición, cuando el gestor de un motor de búsqueda crea en el Estado miembro una sucursal o una filial destinada a garantizar la promoción y la venta de espacios publicitarios propuestos por el mencionado motor y cuya actividad se dirige a los habitantes de este Estado miembro. 3) Los artículos 12, letra b) y 14, párrafo primero, letra a), de la Directiva 95/46 deben interpretarse en el sentido de que, para respetar los derechos que establecen estas disposiciones, siempre que se cumplan realmente los requisitos establecidos en ellos, el gestor de un motor de búsqueda está obligado a eliminar de la lista de resultados obtenida tras una búsqueda efectuada a partir del nombre de una persona vínculos a páginas web, publicadas por terceros y que contienen información relativa a esta persona, también en el supuesto de que este nombre o esta información no se borren previa o simultáneamente de estas páginas web, y, en su caso, aunque la publicación en dichas páginas sea en sí misma lícita. 4) Los artículos 12, letra b), y 14, párrafo primero, letra a), de la Directiva 95/46 deben interpretarse en el sentido de que, al analizar los requisitos de aplicación de estas disposiciones, se tendrá que examinar, en particular, si el interesado tiene derecho a que la información en cuestión relativa a su persona ya no esté, en la situación actual, vinculada a su nombre por una lista de resultados obtenida tras una búsqueda efectuada a partir de su nombre, sin que la apreciación de la existencia de tal derecho presuponga que la inclusión de la información en cuestión en la lista de resultados cause un perjuicio al interesado. Puesto que este puede, habida cuenta de los derechos que le reconocen los artículos 7 y 8 de la Carta, solicitar que la información de que se trate ya no se ponga a disposición del público en general mediante su inclusión en tal lista de resultados, estos derechos prevalecen, en principio, no solo sobre el interés económico del gestor del motor de búsqueda, sino también sobre el interés de dicho público en acceder a la mencionada información en una búsqueda que verse sobre el nombre de esa persona. Sin embargo, tal no sería el caso si resultara, por razones concretas, como el papel desempeñado por el interesado en la vida pública, que la injerencia en sus derechos fundamentales está justificada por el interés preponderante de dicho público en tener, a raíz de esta inclusión, acceso a la información de que se trate". Ver en: https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:62012CJ0131&from=ES consulta realizada el 19 de abril de 2021.

El Derecho al Olvido en el RGPD

El Reglamento Europeo 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (RGPD), viene a derogar la Directiva 95/46/CE -norma que había sustentado la aparición del derecho al olvido- y va a regular el derecho a la supresión de datos.

El artículo 17 del RGPD) consagra el derecho a la supresión de datos o derecho al olvido, en lo siguientes términos:

"Derecho de supresión (el derecho al olvido)

1. El interesado tendrá derecho a obtener sin dilación indebida del responsable del tratamiento la supresión de los datos personales que le conciernan, el cual estará obligado a suprimir sin dilación indebida los datos personales cuando concurra alguna de las circunstancias siguientes:

a) los datos personales ya no sean necesarios en relación con los fines para los que fueron recogidos o tratados de otro modo;

b) el interesado retire el consentimiento en que se basa el tratamiento de conformidad con el artículo 6, apartado 1, letra a), o el artículo 9, apartado 2, letra a), y este no se base en otro fundamento jurídico;

c) el interesado se oponga al tratamiento con arreglo al artículo 21, apartado 1, y no prevalezcan otros motivos legítimos para el tratamiento, o el interesado se oponga al tratamiento con arreglo al artículo 21, apartado 2;

d) los datos personales hayan sido tratados ilícitamente;

e) los datos personales deban suprimirse para el cumplimiento de una obligación legal establecida en el Derecho de la Unión o de los Estados miembros que se aplique al responsable del tratamiento;

f) los datos personales se hayan obtenido en relación con la oferta de servicios de la sociedad de la información mencionados en el artículo 8, apartado 1.

2. Cuando haya hecho públicos los datos personales y esté obligado, en virtud de lo dispuesto en el apartado 1, a suprimir dichos datos, el responsable del tratamiento, teniendo en cuenta la tecnología disponible y el coste de su aplicación, adoptará medidas razonables, incluidas medidas técnicas, con miras a informar a los responsables que estén tratando los datos personales de la solicitud del interesado de supresión de cualquier enlace a esos datos personales, o cualquier copia o réplica de los mismos.

3. Los apartados 1 y 2 no se aplicarán cuando el tratamiento sea necesario:

a) para ejercer el derecho a la libertad de expresión e información;

b) para el cumplimiento de una obligación legal que requiera el tratamiento de datos impuesta por el Derecho de la Unión o de los Estados miembros que se aplique al responsable del tratamiento, o para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable;

c) por razones de interés público en el ámbito de la salud pública de conformidad con el artículo 9, apartado 2, letras h) e i), y apartado 3;

d) con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, de conformidad con el artículo 89, apartado 1, en la medida en que

el derecho indicado en el apartado 1 pudiera hacer imposible u obstaculizar gravemente el logro de los objetivos de dicho tratamiento, o

e) para la formulación, el ejercicio o la defensa de reclamaciones".

Como se puede observar del artículo precedente, es posible distinguir en la configuración del derecho al olvido tres cuestiones importantes. La primera se refiere al derecho de los interesados a obtener en determinadas circunstancias del responsable del tratamiento, sin retraso indebido, la supresión de los datos personales inexactos que le conciernan. De igual forma el responsable del tratamiento se encuentra obligado a suprimir los datos, sin demora alguna en ciertas y determinadas circunstancias previstas en la normativa. La tercera tiene que ver con los límites del derecho a la supresión de datos personales.

De la segunda parte del artículo 17 del RGPD se desprende la obligación en la medida de lo razonable del responsable del tratamiento de notificar la supresión de los datos personales al resto de responsables que estén realizando un tratamiento de dichos datos que se le habían proporcionado, con la finalidad que se tomen medidas oportunas.

El apartado tercero se refiere a las excepciones o limitaciones al derecho al olvido que no es un derecho absoluto. Limitaciones como las que se derivan de la segunda parte del Considerando 65 *in fine* del RGPD;

"… Sin embargo, la retención ulterior de los datos personales debe ser lícita cuando sea necesaria para el ejercicio de la libertad de expresión e información, para el cumplimiento de una obligación legal, para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento, por razones de interés público en el ámbito de la salud pública, con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, o para la formulación, el ejercicio o la defensa de reclamaciones".

De Terwangne define el derecho al olvido como el "derecho de las personas físicas a hacer que se borre la información sobre ellas después de un periodo de tiempo"[206]. De igual forma Dávara Rodríguez señala que el derecho al olvido "es aquel derecho que tiene el titular de un dato a que éste sea borrado o bloqueado, cuando se produzcan determinadas circunstancias y, en particular, que no sea accesible a través de la red de internet"[207].

Parte de la doctrina ha sostenido que el derecho al olvido no constituye un derecho nuevo propiamente tal, sino que sería otra expresión del derecho a la cancelación de datos en el entorno virtual de internet. Autores como Pazos Castro plantean que se ha otorgado un nuevo nombre a derechos ya conocidos como son los de oposición y cancelación, y que este nuevo nombre se emplearía para una aplicación particular de los mismos[208]. Sin embargo, más allá de tales consideraciones y teniendo en cuenta el desarrollo de las tecnologías de la información,

[206] De Terwangne, C. (2012), "Privacidad en Internet y el derecho a ser olvidado/derecho al olvido", Monográfico, VII Congreso Internacional Internet, Derecho y Política. Neutralidad de la red y otros retos para el futuro de Internet, *Revista D'Internet, Dret i Politica (IDP)*, n° 13, p.54.

[207] Dávara Rodríguez, M. (2013), "El derecho al olvido en internet", *La Ley*, año XXXIV, n° 8137, p.2.

[208] Pazos Castro, R. (2015) "El mal llamado derecho al olvido en la era de Internet", *Boletín del Ministerio de Justicia*, N° 2183, año LXIX, p. 40.

las telecomunicaciones y el *Big data,* el derecho al olvido surge como una reconfiguración del derecho de la cancelación de los datos en la Era Digital colocando al titular en una posición de control sobre sus datos personales.

Así, el derecho al olvido se sustenta en los principios derivados de la protección de datos de carácter personal a los que hace referencia el RGPD, como son el principio de calidad del dato[209], el principio de finalidad[210], el principio de proporcionalidad[211] y el principio de consentimiento[212]. Operando el derecho al olvido como un mecanismo que, para el cumplimiento efectivo del principio de finalidad, que establece que los datos personales solo pueden utilizarse para una finalidad concreta y determinada para la que fueron recabados, y ya no siendo necesarios para dichos efectos, procede su cancelación.

Ilustrativo también sobre el contenido y alcance del derecho al olvido es el Considerando 65 del RGPD en su primera parte, del cual se desprende que:

> *"Los interesados deben tener derecho a que se rectifiquen los datos personales que le conciernen y un "derecho al olvido" si la retención de tales datos infringe el presente Reglamento o el Derecho de la Unión o de los Estados miembros aplicable al responsable del tratamiento. En particular, los interesados deben tener derecho a que sus datos personales se supriman y dejen de tratarse si ya no son necesarios para los fines para los que fueron recogidos o tratados de otro modo, si los interesados han retirado su consentimiento para el tratamiento o se oponen al tratamiento de datos personales que les conciernen, o si el tratamiento de sus datos personales incumple de otro modo el presente Reglamento. Este derecho es pertinente en particular si el interesado dio su consentimiento siendo niño y no se es plenamente consciente de los riesgos que implica el tratamiento, y más tarde quiere suprimir tales datos personales,*

[209]Artículo 5.1 "Los datos personales serán d) exactos y, si fuera necesario, actualizados; se adoptarán todas las medidas razonables para que se supriman o rectifiquen sin dilación los datos personales que sean inexactos con respecto a los fines para los que se tratan ("exactitud")".

[210]Artículo 5.1 "Los datos personales serán b) recogidos con fines determinados, explícitos y legítimos, y no serán tratados ulteriormente de manera incompatible con dichos fines; de acuerdo con el artículo 89, apartado 1, el tratamiento ulterior de los datos personales con fines de archivo en interés público, fines de investigación científica e histórica o fines estadísticos no se considerará incompatible con los fines iniciales ("limitación de la finalidad")".

[211]Artículo 5.1 "Los datos personales serán c) adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados ("minimización de datos")".

[212] Artículo 7 "Condiciones para el consentimiento 1. Cuando el tratamiento se base en el consentimiento del interesado, el responsable deberá ser capaz de demostrar que aquel consintió el tratamiento de sus datos personales. 2. Si el consentimiento del interesado se da en el contexto de una declaración escrita que también se refiera a otros asuntos, la solicitud de consentimiento se presentará de tal forma que se distinga claramente de los demás asuntos, de forma inteligible y de fácil acceso y utilizando un lenguaje claro y sencillo. No será vinculante ninguna parte de la declaración que constituya infracción del presente Reglamento. 3. El interesado tendrá derecho a retirar su consentimiento en cualquier momento. La retirada del consentimiento no afectará a la licitud del tratamiento basada en el consentimiento previo a su retirada. Antes de dar su consentimiento, el interesado será informado de ello. Será tan fácil retirar el consentimiento como darlo. 4. Al evaluar si el consentimiento se ha dado libremente, se tendrá en cuenta en la mayor medida posible el hecho de si, entre otras cosas, la ejecución de un contrato, incluida la prestación de un servicio, se supedita al consentimiento al tratamiento de datos personales que no son necesarios para la ejecución de dicho contrato".

especialmente en internet. El interesado debe poder ejercer este derecho, aunque ya no sea un niño...".

Como se ha señalado, el derecho al olvido o supresión surge como una expresión de derechos derivados de la protección de datos ya existentes, o si se quiere, constituye el resultado de la evolución y desarrollo de las nuevas tecnologías, las telecomunicaciones y *Big data* sobre los derechos de cancelación y oposición, comprendidos en los denominados derechos ARCO.

Como señala Álvarez Caro, "el Reglamento reconoce un derecho de los interesados a que sus datos sean suprimidos por el responsable del tratamiento en determinadas circunstancias y salvo que se den otros supuestos contemplados en el ámbito de las excepciones a este derecho. Asimismo, se recoge una obligación de informar a otros responsables del tratamiento que estén tratando los datos, con el fin de que tomen medidas y supriman toda replica, copia o enlace a los mismos"[213].

El Derecho de Portabilidad

Otro derecho, también consagrado por el RGPD, es el denominado derecho a la portabilidad de los datos previsto en los artículo 20:

1. *El interesado tendrá derecho a recibir los datos personales que le incumban, que haya facilitado a un responsable del tratamiento, en un formato estructurado, de uso común y lectura mecánica, y a transmitirlos a otro responsable del tratamiento sin que lo impida el responsable al que se los hubiera facilitado, cuando:*
   a) el tratamiento esté basado en el consentimiento con arreglo al artículo 6, apartado 1, letra a), o el artículo 9, apartado 2, letra a), o en un contrato con arreglo al artículo 6, apartado 1, letra b), y
   b) el tratamiento se efectúe por medios automatizados.
2. *Al ejercer su derecho a la portabilidad de los datos de acuerdo con el apartado 1, el interesado tendrá derecho a que los datos personales se transmitan directamente de responsable a responsable cuando sea técnicamente posible.*
3. *El ejercicio del derecho mencionado en el apartado 1 del presente artículo se entenderá sin perjuicio del artículo 17 [derecho al olvido]. Tal derecho no se aplicará al tratamiento que sea necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento.*
4. *El derecho mencionado en el apartado 1 no afectará negativamente a los derechos y libertades de otros*

Es el derecho a obtener del controlador una copia de los datos que se están procesando de manera electrónica y estructurada, permitiendo un uso posterior por el titular de dichos datos para que ese tratamiento se realice por un tercero. En definitiva, es un derecho del interesado a recibir -bien directamente o por remisión a un tercero- los datos personales que le conciernan.

[213] Álvarez Caro, M. (2015), "Derecho al Olvido en Internet: el nuevo paradigma de la privacidad en la era digital", Reus.

Es importante señalar que los datos deben entregarse en un formato estructurado, de uso común y lectura mecánica.

En definitiva, son dos las vías o formas por las que se ejerce este derecho a la portabilidad; una, que los datos se transmitan al propio interesado, y la otra, que los datos se transmitan a un tercero que especifique el interesado, el que pasa a convertirse en el nuevo responsable del tratamiento de datos.

También es de señalar que este derecho a la portabilidad es compatible cuando sea procedente con el derecho a la supresión de datos personales en el responsable de la base de datos inicial.

El Derecho de Oposición

Por su parte, el derecho de oposición, cambia de forma menos protectora a la prevista inicialmente[214], pues ahora se permite la elaboración de perfiles y en el artículo 21 establece:

1. *El interesado tendrá derecho a oponerse en cualquier momento, por motivos relacionados con su situación particular, a que datos personales que le conciernan sean objeto de un tratamiento basado en lo dispuesto en el artículo 6, apartado 1, letras e) o f)[en interés público o interés legítimo], incluida la elaboración de perfiles sobre la base de dichas disposiciones. El responsable del tratamiento dejará de tratar los datos personales, salvo que acredite motivos legítimos imperiosos para el tratamiento que prevalezcan sobre los intereses, los derechos y las libertades del interesado, o para la formulación, el ejercicio o la defensa de reclamaciones.*
2. *Cuando el tratamiento de datos personales tenga por objeto la mercadotecnia directa, el interesado tendrá derecho a oponerse en todo momento al tratamiento de los datos personales que le conciernan, incluida la elaboración de perfiles en la medida en que esté relacionada con la citada mercadotecnia.*
3. *Cuando el interesado se oponga al tratamiento con fines de mercadotecnia directa, los datos personales dejarán de ser tratados para dichos fines.*

[214] El artículo 13 de la española y derogada Ley Orgánica 5/1999 de Protección de Datos Personales establecía el derecho de oposición en los siguientes términos: *Impugnación de valoraciones.*

1. Los ciudadanos tienen derecho a no verse sometidos a una decisión con efectos jurídicos, sobre ellos o que les afecte de manera significativa, que se base únicamente en un tratamiento de datos destinados a evaluar determinados aspectos de su personalidad.

2. El afectado podrá impugnar los actos administrativos o decisiones privadas que impliquen una valoración de su comportamiento, cuyo único fundamento sea un tratamiento de datos de carácter personal que ofrezca una definición de sus características o personalidad.

3. En este caso, el afectado tendrá derecho a obtener información del responsable del fichero sobre los criterios de valoración y el programa utilizados en el tratamiento que sirvió para adoptar la decisión en que consistió el acto.

4. La valoración sobre el comportamiento de los ciudadanos, basada en un tratamiento de datos, únicamente podrá tener valor probatorio a petición del afectado.

4. *A más tardar en el momento de la primera comunicación con el interesado, el derecho indicado en los apartados 1 y 2 será mencionado explícitamente al interesado y será presentado claramente y al margen de cualquier otra información.*
5. *En el contexto de la utilización de servicios de la sociedad de la información, y no obstante lo dispuesto en la Directiva 2002/58/CE [], el interesado podrá ejercer su derecho a oponerse por medios automatizados que apliquen especificaciones técnicas.*
6. *Cuando los datos personales se traten con fines de investigación científica o histórica o fines estadísticos de conformidad con el artículo 89, apartado 1, el interesado tendrá derecho, por motivos relacionados con su situación particular, a oponerse al tratamiento de datos personales que le conciernan, salvo que sea necesario para el cumplimiento de una misión realizada por razones de interés público.*

También se encuentra previsto en los considerandos del RGPD, en efecto, del considerando 69 se desprende: "…que el interesado debe, sin embargo, tener derecho a oponerse al tratamiento de cualquier dato personal relativo a su situación particular…" y a continuación el considerando 70 dispone que "Si los datos personales son tratados con fines de mercadotecnia directa, el interesado debe tener derecho a oponerse a dicho tratamiento, inclusive a la elaboración de perfiles en la medida en que esté relacionada con dicha mercadotecnia directa, ya sea con respecto a un tratamiento inicial o ulterior, y ello en cualquier momento y sin coste alguno. Dicho derecho debe comunicarse explícitamente al interesado y presentarse claramente y al margen de cualquier otra información".

Por consiguiente, es posible concluir que el derecho de oposición se ejerce cuando este se sustenta en una situación particular del titular de los datos y sobre el tratamiento de datos de dos de las seis razones que el artículo 6 establece para el tratamiento lícito de datos personales: el interés público o el interés legítimo, y más concretamente, cuando la oposición al tratamiento tenga por objeto la mercadotecnia o publicidad directa que es un interés legítimo.

Como es posible advertir, el Reglamento representa un trascendental hito en el desarrollo y la consolidación del derecho a la protección de datos de carácter personal en Europa, pero también para otros países, reforzando las facultades de los autoridades o agencias encargadas de la promoción y regulación de la protección de datos, dando coherencia al sistema normativo europeo e influyendo en las respectivas legislaciones nacionales en la materia.

El Informe de la Comisión del Parlamento Europeo a dos años de la aplicación del RGPD

Abordadas las regulaciones contendidas en el RGPD resulta pertinente destacar que el 24 de junio del año 2020, la Comisión del Parlamento Europea evacuó el informe "La protección de datos como pilar del empoderamiento de los ciudadanos y del enfoque de la UE para la transición digital: dos años de aplicación del Reglamento General de Protección de Datos", el cual también hace referencia a la importancia de "Promover la convergencia y la cooperación

internacional en el ámbito de la protección de datos"[215], lo que evidentemente representa una oportunidad para la regulación que requiere Latinoamérica, en efecto, el señalado informe plantea que el RGPD se ha convertido en un punto de referencia clave a nivel internacional y ha servido de catalizador para que muchos países del mundo consideren la adopción de normas de privacidad modernas, por ejemplo Brasil, publica el 15 de agosto del año 2018 la Ley N° 13.709, Ley General de Protección de Datos, con una vacancia legal de veinticuatro meses, es decir, con entrada en vigencia a partir de agosto del año 2020. O lo ocurrido en Perú mediante el Decreto Legislativo N° 1353, de 7 enero de 2017, por el cual se crea la Autoridad Nacional de Transparencia y Acceso a la Información Pública con el objeto de fortalecer el Régimen de Protección de Datos Personales y la regulación de la gestión de intereses.

El avanzar hacia una mayor convergencia en la regulación del derecho fundamental a la protección de datos de carácter personal abre oportunidades para los países latinoamericanos, que no cuentan en la mayoría de sus ordenamientos jurídicos internos con una normativa efectiva que la regule, pudiendo adaptar a sus respectivas realidades la experiencia de la UE tomando como referencia el RGPD, lo que al mismo tiempo facilitará la circulación e intercambio de datos e información. En este sentido, la Comisión Europea ha intensificado su diálogo en una serie de foros bilaterales, regionales y multilaterales a fin de fomentar una cultura mundial de respeto a la privacidad desarrollando elementos de convergencia entre los distintos sistemas de protección de la privacidad y a los datos de carácter personal.

Se busca promover la convergencia de las normas de protección de datos a nivel internacional como forma de facilitar la circulación de datos y, con ello, el comercio, sobre este punto recordemos que solo tres países latinoamericanos han suscrito el Convenio 108, México el 12 de junio de 2018, luego Uruguay el 10 de octubre de 2018 y luego Argentina, el 19 de septiembre de 2019.

En el señalado informe, la Comisión se compromete a contribuir al desarrollo de marcos jurídicos adecuados con países que realizan intercambio comercial para evitar conflictos normativos apoyando formas eficaces de cooperación, en particular estableciendo las garantías necesarias en materia de protección de datos. La Comisión señala la necesidad de desarrollar instrumentos jurídicos adecuados para establecer formas más estrechas de cooperación y asistencia mutua, permitiendo los intercambios de información.

La Comisión Europea asume en el referido informe y en el contexto del desarrollo de la protección de datos a dos años de la entrada en vigor del RGPD, algunos de los siguientes compromisos:

1. Apoyará los procesos de reforma en curso en terceros países sobre normas de protección de datos nuevas o modernizadas mediante el intercambio de experiencias y mejores prácticas.

2. Evaluará las formas en que podría facilitarse la cooperación entre los operadores privados y las autoridades encargadas de hacer cumplir la ley, en

[215] Página 15, ver:https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52020DC0264&from=EN

particular mediante la negociación de marcos bilaterales y multilaterales para las transferencias de datos en el contexto del acceso de las autoridades extranjeras encargadas de hacer cumplir la ley a las pruebas electrónicas a fin de evitar conflictos normativos, velando al mismo tiempo por la aplicación de garantías adecuadas en materia de protección de datos.

3. Colaborará con organizaciones internacionales y regionales como la *Organización para la Cooperación y el Desarrollo Económicos* (OCDE), la Asociación de Naciones del Sudeste Asiático (ASEAN) o el G-20 para promover la circulación de datos fiables basada en normas estrictas de protección de datos, incluido en el contexto de la iniciativa de "libre circulación de datos con confianza".

4. Creará una "Academia de Protección de Datos" para facilitar y apoyar los intercambios entre reguladores europeos e internacionales.

5. Promoverá la cooperación internacional en materia de cumplimiento de la normativa entre las autoridades de supervisión, incluido mediante la negociación de acuerdos de cooperación y asistencia mutua.

La Protección de Datos Personales en España

Anclaje constitucional

En España, como ya se ha señalado, la Constitución de 1978 establece en su artículo 18.4 que "La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos". Precepto que se ha entendido como la fuente constitucional de la protección de datos como derecho fundamental, intrínsecamente vinculada como ya se ha expuesto al derecho a la intimidad y a la vida privada, pero que jurisprudencialmente se va a conformar un derecho fundamental con una independencia y autonomía propia. En este sentido es esencial la jurisprudencia constitucional que en España sí que es fuente del Derecho[216].

Según Hernández López[217], en la configuración del derecho a la protección de datos como derecho fundamental autónomo, ha sido relevante la posición del Tribunal Constitucional

[216] Véase Goig Martínez, J. M., Núñez Rivero, C. y Núñez Martínez M.A. (2019). *El sistema de fuentes del derecho constitucional en la jurisprudencia del tribunal constitucional español*. Universitas: "la doctrina española ha rechazado la consideración de la jurisprudencia como fuente directa del Derecho y en este mismo sentido se ha manifestado el propio Código Civil. Sin embargo, la Constitución de 1978 y el sistema jurídico subsiguiente han puesto las bases para una diferente valoración de la jurisprudencia constitucional como fuente del Derecho"

[217] Hernández López, J. (2018), "Reglamento General del Protección de Datos. Incluye cronología, webgrafía, bibliografía e índice analítico", Valencia, Tirant lo Blanch.

español, del cual pueden apreciarse en su evolución tres fases o momentos; Una fase inicial (1981-1993), donde se muestra una preocupación por los peligros de las nuevas tecnologías y los derechos fundamentales, cuestión que se expresa por ejemplo en la STC142/1993. Una fase de transición (1993-2000), donde se establece la libertad informática como expresión positiva del derecho a la intimidad. En este periodo la "libertad informática" aparece como la vertiente positiva del derecho a la intimidad, criterio que se expresa en la STC 254/1993. Y finalmente, una fase de reconocimiento pleno (2000-actualidad), en el que se reconoce la protección de datos personales como derecho fundamental autónomo que se expresa con mucha nitidez, como señalamos hace algunas líneas atrás en la STC 292/2000.

Sobre este derecho a la protección de datos de carácter personal, el Tribunal Constitucional Español en STC 96/2012, (Fundamento Jurídico 6), ha señalado que es un derecho fundamental que deriva del artículo 18.4 de la Constitución Española CE y que por consiguiente se garantiza o tutela con el más alto nivel de protección que otorga la Carta, lo que implica que solo puede ser regulado por ley orgánica, según se desprende del artículo 81.1 de la CE, vinculado a todos los poderes públicos, pudiendo ser regulado solo por ley sin alterar su contenido esencial, como se establece en el artículo 53.1 de la CE, otorgando además una tutela judicial efectiva mediante un procedimiento preferente y sumario ante los tribunales de justicia y, en el caso de no obtenerse amparo, a través del recurso de amparo constitucional, tal y como prevé el artículo 53.2 de la Constitución.

Es cierto que con más de una década de antelación[218] ya lo habían previsto las SSTC 290/2000 y 292/2000[219], sin embargo, merece especial atención para estos efectos el voto particular formulado por Jiménez de Parga en la STC 290/2000, en el que comparte el sentido del fallo, pero discrepa señalando que debió establecerse explícitamente que el Tribunal Constitucional reconoce y protege un nuevo derecho, el derecho de la libertad informática, que no figura en el catálogo de derechos fundamentales de la CE. Su voto discrepa de la sentencia, en orden a sostener que el apartado 4 del artículo 18 solo es un simple mandato al legislador para que limite el uso de la informática y por consiguiente el derecho fundamental a la libertad informática, no reconocido explícitamente en la Constitución, el que debe tener como sustento el artículo 10.1 de la CE[220], ya que es un derecho inherente a la dignidad humana. Señala Jiménez de Parga en su voto particular: "A mi entender la libertad informática en cuanto derecho fundamental no recogido expresamente en el texto de 1978 debe tener como eje vertebrador el art. 10.1 CE, ya que es un derecho inherente a la dignidad de la persona. Tal vinculación a la dignidad de la persona proporciona a la libertad informática la debida consistencia constitucional. También son preceptos que facilitan la configuración de la libertad informática los contenidos de los arts. 18.1 (derecho al honor, a la intimidad personal y familiar y a la propia imagen) y 20.1 (libertad de expresión e información) …"

[218] Como complemento de lo señalado, se destaca también la Sentencia del Tribunal Constitucional español N° 254/1993, del 20 de junio, que se refiere a la libertad informática como un derecho fundamental en sí mismo.

[219] Ver en: http://hj.tribunalconstitucional.es/HJ/cs-CZ/Resolucion/Show/SENTENCIA/2000/292

[220] "La dignidad de la persona, los derechos inviolables que le son inherentes, el libre desarrollo de la personalidad, el respeto a la ley y a los derechos de los demás son fundamento del orden político y de la paz social".

Pérez Luño se refiere a la libertad informática como un derecho de la tercera generación de derechos humanos y destaca la conexión entre los derechos a la integridad moral y a la intimidad con las limitaciones al uso de la informática[221].

Murillo de la Cueva afirma que este nuevo derecho se fundamenta en el artículo 18.4 CE y ha de inspirarse en el Convenio 108 del Consejo de Europa de 1981[222].

Sobre el punto, parece acertado concluir que el derecho a la protección de datos es un derecho autónomo sustentado constitucionalmente en el apartado 4 del artículo 18 de la Constitución, pero que como todo derecho fundamental encuentra su fundamento intrínseco en la dignidad humana y por consiguiente también se relaciona con el artículo 10.1 de la CE y con otros derechos fundamentales como el derecho a la intimidad, por lo que no es un derecho absoluto limitando con otros derechos fundamentales. Este derecho, entonces, se configura como un haz de facultades, que se impone a otros deberes jurídicos propios, atribuyendo a su titular control o disposición sobre sus datos personales.

Desarrollo legislativo en España: Tres Leyes Orgánicas de protección de datos personales

Volviendo al derecho a la protección de datos en España y su evolución, el artículo 18.4 CE se desarrolla legislativamente con la Ley Orgánica 5/1992 de 29 de octubre sobre regulación del tratamiento de datos de carácter personal, LORTAD, la que en su artículo 1 ya determinaba su objeto, señalando: "*La presente Ley Orgánica, en desarrollo de la previsto en el apartado 4 del artículo 18 de la Constitución, tiene por objeto limitar el uso de la información y otras técnicas y medios de tratamiento automatizado de los datos de carácter personal para garantizar el honor, la intimidad personal y familiar de las personas físicas y el pleno ejercicio de sus derechos*".

La LORTAD fue derogada por la Ley Orgánica 15/1999 de 13 de diciembre de Protección de Datos de Carácter Personal, LOPD, que adaptó el ordenamiento jurídico español a la Directiva 95/46/CE. La LOPD según su artículo 1 tenía por objeto "*garantizar y proteger, en lo que concierne al tratamiento de los datos personales, las libertades públicas y los derechos fundamentales de las personas físicas, y especialmente de su honor e intimidad personal y familiar*".

La LOPD es derogada por la Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales 3/2018, (LOPDPyGDD), publicada en el Boletín Oficial del Estado (BOE) N°294, de 6 de diciembre de 2018, actualmente vigente y que en su artículo 1 establece su objeto al señalar que persigue: "*Adaptar el ordenamiento jurídico español al Reglamento (UE) 2016/679 del Parlamento Europeo y el Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de sus datos personales y*

[221] Pérez Luño, A. (2006), "*La tercera generación de derechos humanos*", Thomson-Aranzi, Madrid, pp.32-42.

[222] Murillo de la Cueva, L. (1999), "La construcción del derecho a la autodeterminación informativa", *Revista de Estudios Políticos (Nueva época)*, n° 104, abril-junio, p.40.

a la libre circulación de estos datos, y completar sus disposiciones. El derecho fundamental de las personas físicas a la protección de datos personales, amparado por el artículo 18.4 de la Constitución, se ejercerá con arreglo a lo establecido en el Reglamento (UE) 2016/679 y en esta ley orgánica". Además de "*Garantizar los derechos digitales de la ciudadanía conforme al mandato establecido en el artículo 18.4 de la Constitución*".

Esta ley se estructura sobre un Preámbulo de cinco partes, en 96 artículos contenidos en diez títulos, veintidós disposiciones adicionales, seis disposiciones transitorias, una disposición derogatoria y dieciséis disposiciones finales.

El título I relativo a las disipaciones generales; el título II se refiere a los principios de protección de datos; el título III aborda los derechos de las personas; el título IV recoge las disposiciones aplicables a tratamientos concretos; el título V se refiere al responsable y al encargado del tratamiento; el título VI aborda las transferencias internacionales de datos; el título VII se dedica a las autoridades de protección de datos; el título VIII se refiere a los procedimientos en caso de posible vulneración de la normativa de protección de datos; el título IX regula el régimen sancionador y el título X reconoce y garantiza un conjunto de derechos digitales.

Las disposiciones adicionales abordan materias relacionadas con las medidas de seguridad en el ámbito del sector público, protección de datos, transparencia y acceso a la información pública, computo de plazos, autorización judicial en materia de transferencias internacionales de datos, la protección frente a prácticas abusivas que pudieran desarrollar ciertos operadores, o los aspectos relacionados a tratamientos de datos de la salud, entre otros contenidos.

Las disposiciones transitorias están abocadas entre otras materias al estatuto de la Agencia Española de Protección de Datos. Luego se establecen las disposiciones finales sobre los preceptos con carácter de ley ordinaria y la entrada en vigor.

No es un derecho absoluto. La necesaria proporcionalidad

Sobre el carácter no absoluto del derecho a la protección de datos hay que tener en consideración el denominado principio de proporcionalidad, que permita mantener un adecuado equilibrio entre este derecho y otros derechos fundamentales, así entonces la proporcionalidad tiene que ver con evaluar si la finalidad que se persigue se puede conseguir por otros medios o haciendo uso de tecnologías menos invasivas, o bien aplicando otros medios de tratamiento de datos personales.

La Agencia Española de Protección de Datos establece un juicio de proporcionalidad para evaluar si el tratamiento de datos personales afecta otros derechos fundamentales, estableciendo tres puntos; 1. Juicio de idoneidad, esto es si la medida puede conseguir el objetivo propuesto; 2. Juicio de necesidad, es decir, si además es necesario, en el sentido de que no existe otra más moderada para conseguir este propósito con la misma eficiencia; 3. Juicio de proporcionalidad en sentido estricto, es decir si la medida es ponderada o equilibrada,

porque se derivan más beneficios o ventajas para el interés general que los perjuicios sobre otros bienes o valores en conflicto[223].

Innovaciones en la normativa española de protección de datos personales.

Solo a modo referencial algunas de las innovaciones que esta Ley Orgánica incorpora adaptándose a la nueva normativa europea en la materia, concretamente al RGPD, son las siguientes:

La LOPDPyGDD, en el Título III se refiere a los derechos de las personas al igual que el RGPD, que lo hace en el Capítulo III, ambas normas se complementan para regular los derechos de las personas, con contínuas referencias en la ley española al reglamento europeo.

Cabe destacar que la ley introduce innovaciones en los derechos de las personas, tales como: en el derecho a ser informado del artículo 11, en el ejercicio de los derechos del artículo 12[224] y en el derecho de acceso, en particular del artículo 13[225]. A ello se añade otras cuestiones innovadoras como la obligación de un responsable de protección de datos en las organizaciones.

Derecho a ser informado con transparencia

El derecho a ser informado del artículo 11 incorpora el principio de transparencia entendida como comprensibilidad, algo que crea una cierta disfunción en este concepto con el que se encuentra en la Ley 19/2013 de Transparencia, Acceso a la Información Pública y Buen Gobierno. El principio de transparencia "exige que la información sea concisa, fácilmente accesible y fácil de entender, y que se utilice un leguaje claro y sencillo, y, además, en su caso,

---

[223] Ver Guía Práctica para las evaluaciones de impacto en la protección de datos sujetas al RGPD, de la Agencia Española de Protección de datos, p.20. consulta realizada el 23 de abril de 2020 en: https://www.aepd.es/sites/default/files/2019-09/guia-evaluaciones-de-impacto-rgpd.pdf.

[224] Artículo l12 LO 3/2018 "Disposiciones generales sobre ejercicio de los derechos. 1. Los derechos reconocidos en los artículos 15 a 22 del Reglamento (UE) 2016/679, podrán ejercerse directamente o por medio de representante legal o voluntario. 2. El responsable del tratamiento estará obligado a informar al afectado sobre los medios a su disposición para ejercer los derechos que le corresponden. Los medios deberán ser fácilmente accesibles para el afectado. El ejercicio del derecho no podrá ser denegado por el solo motivo de optar el afectado por otro medio. 3. El encargado podrá tramitar, por cuenta del responsable, las solicitudes de ejercicio formuladas por los afectados de sus derechos si así se estableciere en el contrato o acto jurídico que les vincule. 4. La prueba del cumplimiento del deber de responder a la solicitud de ejercicio de sus derechos formulado por el afectado recaerá sobre el responsable. 5. Cuando las leyes aplicables a determinados tratamientos establezcan un régimen especial que afecte al ejercicio de los derechos previstos en el Capítulo III del Reglamento (UE) 2016/679, se estará a lo dispuesto en aquellas. 6. En cualquier caso, los titulares de la patria potestad podrán ejercitar en nombre y representación de los menores de catorce años los derechos de acceso, rectificación, cancelación, oposición o cualesquiera otros que pudieran corresponderles en el contexto de la presente ley orgánica. 7. Serán gratuitas las actuaciones llevadas a cabo por el responsable del tratamiento para atender las solicitudes de ejercicio de estos derechos, sin perjuicio de lo dispuesto en los artículos 12.5 y 15.3 del Reglamento (UE) 2016/679 y en los apartados 3 y 4 del artículo 13 de esta ley orgánica".

[225]

se visualice"[226]. Es cierto que el derecho a ser informado ya existía en la normativa anterior, pero ahora el artículo 11 establece :

> *"Transparencia e información al afectado.*
> *1. Cuando los datos personales sean obtenidos del afectado el responsable del tratamiento podrá dar cumplimiento al deber de información establecido en el artículo 13 del Reglamento (UE) 2016/679 facilitando al afectado la información básica a la que se refiere el apartado siguiente e indicándole una dirección electrónica u otro medio que permita acceder de forma sencilla e inmediata a la restante información.*
> *2. La información básica a la que se refiere el apartado anterior deberá contener, al menos:*
> *a) La identidad del responsable del tratamiento y de su representante, en su caso.*
> *b) La finalidad del tratamiento*
> *c) La posibilidad de ejercer los derechos establecidos en los artículos 15 a 22 del Reglamento (UE) 2016/679. Si los datos obtenidos del afectado fueran a ser tratados para la elaboración de perfiles, la información básica comprenderá asimismo esta circunstancia. En este caso, el afectado deberá ser informado de su derecho a oponerse a la adopción de decisiones individuales automatizadas que produzcan efectos jurídicos sobre él o le afecten significativamente de modo similar, cuando concurra este derecho de acuerdo con lo previsto en el artículo 22 del Reglamento (UE) 2016/679.*
> *3. Cuando los datos personales no hubieran sido obtenidos del afectado, el responsable podrá dar cumplimiento al deber de información establecido en el artículo 14 del Reglamento (UE) 2016/679 facilitando a aquel la información básica señalada en el apartado anterior, indicándole una dirección electrónica u otro medio que permita acceder de forma sencilla e inmediata a la restante información. En estos supuestos, la información básica incluirá también:*
> *a) Las categorías de datos objeto de tratamiento.*
> *b) Las fuentes de las que procedieran los datos".*

Derecho de acceso

El derecho de acceso del artículo 13 se va a completar estableciendo cautelas en favor del responsable del tratamiento: posibilidad de solicitud de aclaración de una solicitud de acceso, establecimiento de un acceso remoto directo y seguro, si el coste es desproporcionado, el solicitante debe pagar el coste excesivo,

[226] Punto 58 del Reglamento (UE) 2016/679.

"Derecho de acceso.

1. *El derecho de acceso del afectado se ejercitará de acuerdo con lo establecido en el artículo 15 del Reglamento (UE) 2016/679. Cuando el responsable trate una gran cantidad de datos relativos al afectado y este ejercite su derecho de acceso sin especificar si se refiere a todos o a una parte de los datos, el responsable podrá solicitarle, antes de facilitar la información, que el afectado especifique los datos o actividades de tratamiento a los que se refiere la solicitud.*
2. *El derecho de acceso se entenderá otorgado si el responsable del tratamiento facilitara al afectado un sistema de acceso remoto, directo y seguro a los datos personales que garantice, de modo permanente, el acceso a su totalidad. A tales efectos, la comunicación por el responsable al afectado del modo en que este podrá acceder a dicho sistema bastará para tener por atendida la solicitud de ejercicio del derecho. No obstante, el interesado podrá solicitar del responsable la información referida a los extremos previstos en el artículo 15.1 del Reglamento (UE) 2016/679 que no se incluyese en el sistema de acceso remoto.*
3. *A los efectos establecidos en el artículo 12.5 del Reglamento (UE) 2016/679 se podrá considerar repetitivo el ejercicio del derecho de acceso en más de una ocasión durante el plazo de seis meses, a menos que exista causa legítima para ello.*
4. *Cuando el afectado elija un medio distinto al que se le ofrece que suponga un coste desproporcionado, la solicitud será considerada excesiva, por lo que dicho afectado asumirá el exceso de costes que su elección comporte. En este caso, solo será exigible al responsable del tratamiento la satisfacción del derecho de acceso sin dilaciones indebidas".*

Designación de un Delegado de Protección de Datos

También introduce la personalización de la responsabilidad de la protección de datos personales en las organizaciones mediante el Delegado de Protección de Datos Personales. Es una parte de lo que López Calvo llama "la diligencia como nuevo paradigma"[227]. Se establece la obligación de designar a un Delegado de Protección de Datos, en consonancia con el artículo 37 del RGPD. La ley dispone una serie de supuestos concretos donde es obligatorio la designación de esta nueva figura. Entre estos supuestos cabe destacar, entre otros -de los 16 citados en el artículo 34 de la ley: los colegios profesionales, los centros docentes, los establecimientos financieros y de crédito, las entidades aseguradoras y reaseguradoras, las entidades que desarrollen actividades de publicidad y prospección comercial, las empresas de seguridad privada, las federaciones deportivas cuando traten datos de menores de edad o los centros sanitarios obligados al mantenimiento de las historias clínicas. En este último supuesto es importante aclarar que existe una excepción, donde no es necesaria la designación de un Delegado de Protección de Datos cuando los profesionales de la salud ejerzan su actividad a título individual. Aunque no sea obligatorio el uso de esta figura en una entidad u organización, toda aquella que lo desee podrá designar un delegado de protección de datos forma voluntaria.

[227] López Calvo, J. (2017) *Comentarios al Reglamento Europeo de Protección de Datos.* Madrid, Sepin. Págs. 81 y siguientes.

Tratamiento de datos de contacto de empresarios y profesionales

El artículo 19 de la ley recoge el tratamiento de datos de contacto, de empresarios individuales y de profesionales liberales. Lo que regula este artículo es que se podrán tratar los datos de contacto, así como los datos relativos a las funciones o puestos desempeñados por personas físicas cuando se cumplan dos requisitos: primero, que el tratamiento se refiera únicamente a los datos necesarios para su localización profesional, y segundo, que la finalidad del tratamiento sea únicamente mantener relaciones de cualquier índole con la persona jurídica en la que el afectado preste sus servicios. Dicho artículo 19 indica:

> *Tratamiento de datos de contacto de empresarios individuales y de profesionales liberales.*
>
> *1. Salvo prueba en contrario, se presumirá amparado en lo dispuesto en el artículo 6.1.f) del Reglamento (UE) 2016/679 el tratamiento de los datos de contacto y en su caso los relativos a la función o puesto desempeñado de las personas físicas que presten servicios en una persona jurídica siempre que se cumplan los siguientes requisitos: a) Que el tratamiento se refiera únicamente a los datos necesarios para su localización profesional. b) Que la finalidad del tratamiento sea únicamente mantener relaciones de cualquier índole con la persona jurídica en la que el afectado preste sus servicios.*
>
> *2. La misma presunción operará para el tratamiento de los datos relativos a los empresarios individuales y a los profesionales liberales, cuando se refieran a ellos únicamente en dicha condición y no se traten para entablar una relación con los mismos como personas físicas.*
>
> *3. Los responsables o encargados del tratamiento a los que se refiere el artículo 77.1 de esta ley orgánica podrán también tratar los datos mencionados en los dos apartados anteriores cuando ello se derive de una obligación legal o sea necesario para el ejercicio de sus competencias".*

Derechos digitales

A ello se añaden los Derechos Digitales, "preexistentes, seminuevos o nuevos", en palabras de García Mexia[228], que se encuentran recogidos en el Título X de la ley, concretamente en los artículos 79 al 97, bajo el título "Garantía de los derechos digitales".

Se trata de un añadido a la protección de datos personales[229]. Entre estos derechos podemos destacar aquellos que van a establecer la relación entre la persona y el entorno digital: el derecho a la neutralidad en Internet en el artículo 80, el derecho de acceso universal en el artículo 81, a la seguridad digital en el artículo 82 y a la educación digital en el 83.

En el ámbito laboral nos encontramos con el artículo 88 con derecho a la desconexión digital en el ámbito de la relación laboral, en los artículos 89 y 90 trata del derecho a la intimidad de

[228] García Mexia, P. (2019) "Los derechos digitales en la nueva ley de datos. ¿valor simbólico u operatividad real?" en *Otro Sí* . Colegio de Abogados de Madrid. Páginas 30-32

[229] Puede consultarse la revista del Ilustre Colegio de Abogados de Madrid (2019) *Otrosí.net* Nº 3 La abogacía en la era digital. Dossier sobre derechos digitales. https://www.otrosi.net/hemeroteca/numero-3-2019-7a-epoca

los trabajadores en lo concerniente al uso de dispositivo grabación de imagen y/o sonido, así como sistemas de geolocalización.

Derecho a la neutralidad en Internet

Se trata del derecho al tratamiento equitativo y no discriminatorio del tráfico en la prestación de servicios de acceso a Internet. Algo que implica una obligación de las grandes empresas que en el mundo de las telecomunicaciones ofrecen servicios. Esas empresas han de tratar el tráfico en Internet de manera equitativa, sin discriminación, sin restricciones o interferencias con independencia de quién sea el emisor y el receptor de la comunicación, del contenido, de las aplicaciones o servicios utilizados -de tal o cual compañía-, de los equipos y aparatos. Las empresas no pueden bloquear, ralentizar, alterar, restringir, interferir, degradar contenidos, aplicaciones o servicios concretos[230]. En definitiva, los proveedores de servicios de Internet proporcionarán una oferta transparente de servicios sin discriminación por motivos técnicos o económicos. El citado artículo 80 establece:

Derecho a la neutralidad de Internet.
Los usuarios tienen derecho a la neutralidad de Internet. Los proveedores de servicios de Internet proporcionarán una oferta transparente de servicios sin discriminación por motivos técnicos o económicos.

La implicación del derecho a la protección de datos se encuentra en el hecho que las empresas con servicios en Internet captan mucha información que les permite conocer a los usuarios. El empleo de esa información puede suponer discriminación, por lo que se prohíbe.

Derecho de acceso universal

De alguna forma relacionado con el anterior derecho al prohibir la discriminación en razón de las condiciones del usuario. Se trata de un derecho ya recogido en la Ley española 32/2003 General de Telecomunicaciones que ser refería a un "Servicio universal" como un conjunto de servicios cuya prestación se garantiza para todos los usuarios finales con independencia de su localización geográfica, con una calidad determinada y un precio asequible. Condiciones estas últimas que se establecerían en función de la evolución de las infraestructuras de telecomunicaciones. El citado artículo 81 establece

"Derecho de acceso universal a Internet.
1. Todos tienen derecho a acceder a Internet independientemente de su condición personal, social, económica o geográfica.
2. Se garantizará un acceso universal, asequible, de calidad y no discriminatorio para toda la población.
3. El acceso a Internet de hombres y mujeres procurará la superación de la brecha de género tanto en el ámbito personal como laboral.

[230] Fuertes, M. (2019) "En defensa de la neutralidad en la Red" en *Otro Sí* . Colegio de Abogados de Madrid. Páginas 32-33

4. *El acceso a Internet procurará la superación de la brecha generacional mediante acciones dirigidas a la formación y el acceso a las personas mayores.*
5. *La garantía efectiva del derecho de acceso a Internet atenderá la realidad específica de los entornos rurales.*
6. *El acceso a Internet deberá garantizar condiciones de igualdad para las personas que cuenten con necesidades especiales"*.

Este derecho se completaría con el derecho a la educación digital recogido en el artículo 83 de la misma Ley Orgánica 3/2018.

Derecho a la seguridad digital

El artículo 82 va a establecer otro derecho que a nuestro juicio también es prestacional y que completa el derecho de acceso, el derecho a no ser discriminado por razones técnicas, económicas, sociales… (derecho a la neutralidad) :

Derecho a la seguridad digital. Los usuarios tienen derecho a la seguridad de las comunicaciones que transmitan y reciban a través de Internet. Los proveedores de servicios de Internet informarán a los usuarios de sus derechos.

Derecho a la desconexión digital en el ámbito laboral

Ya en el ámbito laboral el derecho a la desconexión digital, regulado en el artículo 88 y posteriormente en el artículo 20 bis del Estatuto de los Trabajadores y en el 18 del Real Decreto-Ley 28/2020, de trabajo a distancia. Regulación imprescindible por el necesario teletrabajo que se implantó durante la Pandemia del Covid19. Dicho artículo 88 establece

1. *Los trabajadores y los empleados públicos tendrán derecho a la desconexión digital a fin de garantizar, fuera del tiempo de trabajo legal o convencionalmente establecido, el respeto de su tiempo de descanso, permisos y vacaciones, así como de su intimidad personal y familiar.*
2. *Las modalidades de ejercicio de este derecho atenderán a la naturaleza y objeto de la relación laboral, potenciarán el derecho a la conciliación de la actividad laboral y la vida personal y familiar y se sujetarán a lo establecido en la negociación colectiva o, en su defecto, a lo acordado entre la empresa y los representantes de los trabajadores.*
3. *El empleador, previa audiencia de los representantes de los trabajadores, elaborará una política interna dirigida a trabajadores, incluidos los que ocupen puestos directivos, en la que definirán las modalidades de ejercicio del derecho a la desconexión y las acciones de formación y de sensibilización del personal sobre un uso razonable de las herramientas tecnológicas que evite el riesgo de fatiga informática. En particular, se preservará el derecho a la desconexión digital en los supuestos de realización total o parcial del trabajo a distancia, así como en el domicilio del empleado vinculado al uso con fines laborales de herramientas tecnológicas"*.

Derechos a la intimidad frente al uso de dispositivos de videovigilancia y de grabación de sonidos en el lugar de trabajo

Más ligados a la protección de datos se encuentra este derecho recogido en el artículo 88

1. *Los empleadores podrán tratar las imágenes obtenidas a través de sistemas de cámaras o videocámaras para el ejercicio de las funciones de control de los trabajadores o los empleados públicos previstas, respectivamente, en el artículo 20.3 del Estatuto de los Trabajadores y en la legislación de función pública, siempre que estas funciones se ejerzan dentro de su marco legal y con los límites inherentes al mismo. Los empleadores habrán de informar con carácter previo, y de forma expresa, clara y concisa, a los trabajadores o los empleados públicos y, en su caso, a sus representantes, acerca de esta medida. En el supuesto de que se haya captado la comisión flagrante de un acto ilícito por los trabajadores o los empleados públicos se entenderá cumplido el deber de informar cuando existiese al menos el dispositivo al que se refiere el artículo 22.4 de esta ley orgánica.*
2. *En ningún caso se admitirá la instalación de sistemas de grabación de sonidos ni de videovigilancia en lugares destinados al descanso o esparcimiento de los trabajadores o los empleados públicos, tales como vestuarios, aseos, comedores y análogos.*
3. *La utilización de sistemas similares a los referidos en los apartados anteriores para la grabación de sonidos en el lugar de trabajo se admitirá únicamente cuando resulten relevantes los riesgos para la seguridad de las instalaciones, bienes y personas derivados de la actividad que se desarrolle en el centro de trabajo y siempre respetando el principio de proporcionalidad, el de intervención mínima y las garantías previstas en los apartados anteriores. La supresión de los sonidos conservados por estos sistemas de grabación se realizará atendiendo a lo dispuesto en el apartado 3 del artículo 22 de esta ley"*

Derecho a la intimidad ante la utilización de sistemas de geolocalización en el ámbito laboral

El uso de localizadores GPS en vehículos de la empresa o en el propio teléfono que usa el trabajador se autoriza siempre que se avise su uso y se permita el ejercicio de las facultades típicas en la protección de datos personales (acceso, rectificación, limitación del tratamiento y supresión)

1. *Los empleadores podrán tratar los datos obtenidos a través de sistemas de geolocalización para el ejercicio de las funciones de control de los trabajadores o los empleados públicos previstas, respectivamente, en el artículo 20.3 del Estatuto de los Trabajadores y en la legislación de función pública, siempre que estas funciones se ejerzan dentro de su marco legal y con los límites inherentes al mismo.*
2. *Con carácter previo, los empleadores habrán de informar de forma expresa, clara e inequívoca a los trabajadores o los empleados públicos y, en su caso, a sus representantes, acerca de la existencia y características de estos dispositivos. Igualmente deberán informarles acerca del posible ejercicio de los derechos de acceso, rectificación, limitación del tratamiento y supresión".*

Derecho al olvido

Ya nos hemos referido precedentemente al derecho al olvido que se establece en el artículo 17 del RGPDP. No es el momento de un trabajo de conexión y estudio de los derechos derivados de la protección de datos, olvido, actualización, rectificación… solo de su somera exposición. Como manifiesta Sánchez de Diego (2019) "el derecho a la actualización de informaciones en medios digitales (artículo 86) precisa de un deslinde con el derecho de rectificación en Internet (artículo 85) y el derecho al olvido/supresión del artículo 15, derecho al olvido en búsquedas en Internet del artículo 93 y, el derecho al olvido en redes sociales y servicios equivalentes del artículo 94)"[231]. Derecho que ligado a la protección de datos, cobra un especial significado en un futuro próximo. En la Ley Orgánica 3/2018 se encuentra en los artículo 93 y 94. El derecho al olvido presenta una regulación doble en la ley: una regulación de carácter general establecida en el artículo 15 como derecho de supresión en consonancia con el 17 del RGPDP y, otra de los derechos en el entorno digital que en realidad son manifestaciones concretas del derecho al olvido en los procesos de búsqueda en información en Internet del artículo 93 y :

Derecho al olvido en búsquedas de Internet.

1. Toda persona tiene derecho a que los motores de búsqueda en Internet eliminen de las listas de resultados que se obtuvieran tras una búsqueda efectuada a partir de su nombre los enlaces publicados que contuvieran información relativa a esa persona cuando fuesen inadecuados, inexactos, no pertinentes, no actualizados o excesivos o hubieren devenido como tales por el transcurso del tiempo, teniendo en cuenta los fines para los que se recogieron o trataron, el tiempo transcurrido y la naturaleza e interés público de la información.

Del mismo modo deberá procederse cuando las circunstancias personales que en su caso invocase el afectado evidenciasen la prevalencia de sus derechos sobre el mantenimiento de los enlaces por el servicio de búsqueda en Internet.

Este derecho subsistirá aun cuando fuera lícita la conservación de la información publicada en el sitio web al que se dirigiera el enlace y no se procediese por la misma a su borrado previo o simultáneo.

2. El ejercicio del derecho al que se refiere este artículo no impedirá el acceso a la información publicada en el sitio web a través de la utilización de otros criterios de búsqueda distintos del nombre de quien ejerciera el derecho.,

Y el derecho al olvido en redes sociales del artículo 94:

Derecho al olvido en servicios de redes sociales y servicios equivalentes.

1. Toda persona tiene derecho a que sean suprimidos, a su simple solicitud, los datos personales que hubiese facilitado para su publicación por servicios de redes sociales y servicios de la sociedad de la información equivalentes.

2. Toda persona tiene derecho a que sean suprimidos los datos personales que le conciernan y que hubiesen sido facilitados por terceros para su publicación por los servicios de redes sociales y servicios de la sociedad de la información equivalentes cuando fuesen inadecuados, inexactos, no pertinentes, no actualizados o excesivos o

[231] Sánchez de Diego Fernández de la Riva, M. (2019) Dudas sobre el derecho a la actualización de informaciones en medios digitales" en en *Otro Sí* . Colegio de Abogados de Madrid. Páginas 46-47.

hubieren devenido como tales por el transcurso del tiempo, teniendo en cuenta los fines para los que se recogieron o trataron, el tiempo transcurrido y la naturaleza e interés público de la información.

Del mismo modo deberá procederse a la supresión de dichos datos cuando las circunstancias personales que en su caso invocase el afectado evidenciasen la prevalencia de sus derechos sobre el mantenimiento de los datos por el servicio.

Se exceptúan de lo dispuesto en este apartado los datos que hubiesen sido facilitados por personas físicas en el ejercicio de actividades personales o domésticas.

4. *En caso de que el derecho se ejercitase por un afectado respecto de datos que hubiesen sido facilitados al servicio, por él o por terceros, durante su minoría de edad, el prestador deberá proceder sin dilación a su supresión por su simple solicitud, sin necesidad de que concurran las circunstancias mencionadas en el apartado 2.*

Derecho al testamento digital.

Otra faceta importante del tiempo en los derechos digitales la encontramos en este derecho que señala que los datos personales subsisten incluso una vez fallecida la persona. El artículo 96 de la Ley Orgánica 3/2018 establece:

1. *El acceso a contenidos gestionados por prestadores de servicios de la sociedad de la información sobre personas fallecidas se regirá por las siguientes reglas:*

   a) Las personas vinculadas al fallecido por razones familiares o de hecho, así como sus herederos podrán dirigirse a los prestadores de servicios de la sociedad de la información al objeto de acceder a dichos contenidos e impartirles las instrucciones que estimen oportunas sobre su utilización, destino o supresión. Como excepción, las personas mencionadas no podrán acceder a los contenidos del causante, ni solicitar su modificación o eliminación, cuando la persona fallecida lo hubiese prohibido expresamente o así lo establezca una ley. Dicha prohibición no afectará al derecho de los herederos a acceder a los contenidos que pudiesen formar parte del caudal relicto.

   b) El albacea testamentario, así como aquella persona o institución a la que el fallecido hubiese designado expresamente para ello también podrá solicitar, con arreglo a las instrucciones recibidas, el acceso a los contenidos con vistas a dar cumplimiento a tales instrucciones.

   c) En caso de personas fallecidas menores de edad, estas facultades podrán ejercerse también por sus representantes legales o, en el marco de sus competencias, por el Ministerio Fiscal, que podrá actuar de oficio o a instancia de cualquier persona física o jurídica interesada.

   d) En caso de fallecimiento de personas con discapacidad, estas facultades podrán ejercerse también, además de por quienes señala la letra anterior, por quienes hubiesen sido designados para el ejercicio de funciones de apoyo si tales facultades se entendieran comprendidas en las medidas de apoyo prestadas por el designado.

2. *Las personas legitimadas en el apartado anterior podrán decidir acerca del mantenimiento o eliminación de los perfiles personales de personas fallecidas en redes sociales o servicios equivalentes, a menos que el fallecido hubiera decidido acerca de esta circunstancia, en cuyo caso se estará a sus instrucciones. El responsable del*

servicio al que se le comunique, con arreglo al párrafo anterior, la solicitud de eliminación del perfil deberá proceder sin dilación a la misma.

3. *Mediante real decreto se establecerán los requisitos y condiciones para acreditar la validez y vigencia de los mandatos e instrucciones y, en su caso, el registro de los mismos, que podrá coincidir con el previsto en el artículo 3 de esta ley orgánica.*
4. *Lo establecido en este artículo en relación con las personas fallecidas en las comunidades autónomas con derecho civil, foral o especial, propio se regirá por lo establecido por estas dentro de su ámbito de aplicación".*

Consideraciones finales del Capítulo

De todo lo expuesto en este capítulo, es posible realizar a lo menos las siguientes tres consideraciones finales;

1. Existe una evidente raíz normativa común entre el derecho a la intimidad, a la protección y respeto a la vida privada, a la privacidad y a la protección de datos, pero el vertiginoso desarrollo de las tecnologías de la información, así como la relevancia del almacenamiento de los datos y su tratamiento tanto al interior de los Estados, en los sectores públicos y privados, como su transferencia a otros países, han impulsado desde hace ya varias décadas la configuración de un nuevo derecho fundamental, cual es la protección de datos personales, el que tiene una independencia y autonomía propias, las que no solo constituyen un límite para que los datos del interesado o titular no puedan ser tratados sin su consentimiento, sino que, además, le permiten disponer libremente de los mismos.

2. La aprobación primero, y luego la entrada en vigor del Reglamento General de Protección de Datos de la UE, no solo contribuyó a profundizar la uniformidad de Europa en materia de protección de datos, si no que incentivo dicho avance hacia otras latitudes, promoviendo la consolidación de este derecho fundamental, reconocido constitucionalmente en otros países, tal como en el año 2018 ocurrió en el caso chileno.

3. Finalmente, la entrada en vigor de la Ley Orgánica 3/2018 sobre protección de datos personales y garantía de los derechos digitales, viene a ajustar la legislación española con la actual normativa europea, ampliando además la configuración de los denominados derechos ARCO, incorporando y remitiéndose al RGPD en lo referido a nuevos derechos digitales, como los de portabilidad, límites al tratamiento y el denominado derecho al olvido que presenta interesantes facetas que deberán ser interpretadas como un derecho vinculado al derecho a la protección de datos personales. De alguna forma se construye un sistema complejo de derechos y obligaciones en torno a la utilización de datos personales en el entorno digital.

CAPÍTULO II

LA TUTELA DE LA PROTECCIÓN DE DATOS Y SU JURISPRUDENCIA ANTE EL TRIBUNAL DE JUSTICIA DE LA UNIÓN EUROPEA

Protección de los Derechos Fundamentales. Garantías en sentido amplio.

La protección de datos, como todo derecho fundamental, debe estar en permanente actualización. Parece unánime en la doctrina que entiende que "los derechos fundamentales y las libertades públicas no constituyen un numerus clausus". En palabras de Desantes, "el elenco de derechos humanos ha de ser necesariamente abierto"[232]. "El catálogo de derechos fundamentales no está ni cerrado, porque es susceptible de nuevas incorporaciones y no es estático porque los derechos fundamentales evolucionan con el tiempo y el espacio"[233]. Como tal, además de actualizarse en cuanto a su contenido y alcance, los derechos fundamentales precisan de una tutela que los hagan eficaces y no meramente programáticos.

Y esto ocurre también en el derecho a la protección de datos que requiere también de tutela y acciones efectivas para su efectivo desarrollo. Así, con el objetivo de asegurar el cumplimiento de los derechos, los ordenamientos jurídicos han establecido elementos de garantía en sentido amplio. El concepto de garantía en sentido amplio se entiende como aquellos mecanismos de protección de un derecho, sean o no jurisdiccionales, de entre los cuales es posible distinguir tres tipos o medios para promover la plena vigencia de tales derechos: garantías normativas, procedimientos jurídicos específicos y garantías institucionales (autoridad de control).

Garantías normativas

Los primeros denominan garantías normativas al reconocimiento expreso de los derechos, las que se insertan en las constituciones y tienen un desarrollo jurídico en la ley. Es lo que ocurre con las denominadas garantías constitucionales, que en el caso chileno están contenidas en el capítulo III de la Carta, artículo 19 numeral primero al veintiséis.

Como ya se abordó en el capítulo anterior, hasta el año 2018 la protección de datos personales en el sistema constitucional chileno se encontraba subsumida, es decir, era un derecho

[232] Sánchez de Diego, Fernández de la Riva, M. (2013). "Transparencia y acceso a la información pública ¿son lo mismo? Por un derecho fundamental a acceder a la información pública" en Corredoira L. y Cotino L. (coordinadores), "*Libertad de expresión e información en Internet: amenazas y protección de los derechos personales"*, Madrid, Centro de Estudios Políticos y Constitucionales, pp. 285- 324.

[233] Sánchez de Diego Fernández de la Riva, M. (2022) El derecho de acceso a la información. Un tortuoso camino.. Madrid. Editorial Fragua. pp. 61

fundamental implícito en el número cuarto del artículo 19 de la Constitución[234]. Después de cuatro años de tramitación legislativa, se publicó en el Diario Oficial el 16 de junio de 2018 la Ley 21.096, que consagró explícitamente la protección de datos personales como una garantía constitucional inmersa en el citado artículo, quedando finalmente de la siguiente forma: "El respeto y protección a la vida privada y a la honra de la persona y su familia y, asimismo la protección de sus datos personales. El tratamiento y protección de estos datos se efectuará en la forma y condiciones que determine la ley".

De esta forma, se elaboró una redacción que incluye la protección de datos personales dentro del numeral cuarto que consagra el derecho a la privacidad y a la honra, que con la expresión "asimismo", antes de establecer un nuevo derecho, consignó la existencia de un derecho con autonomía, pero amparado por la misma acción que tutela al numeral cuarto, esto es, el recurso de protección regulado en el artículo 20 del texto constitucional. La expresión "asimismo", entonces, expresa la intención del constituyente de generar un derecho independiente y diferente a la privacidad y la honra, pero que tendrá la misma protección que dichos derechos, para luego remitir a la ley su regulación. Sobre este último aspecto, el de la remisión legislativa, es fácil advertir que la Ley 19.628, del año 1999, que regula la protección de datos personales en Chile, requiere necesariamente ser reformulada, ya que esta última modificación constitucional exige una actualización de esta, cuestión que abordaremos en profundidad en los siguientes capítulos.

Procedimientos jurídicos específicos

Un segundo mecanismo para asegurar la vigencia de los derechos lo constituyen los procedimientos jurídicos específicos, en este caso la ley 19.628 chilena consagra en su art. 16 un procedimiento para que los afectados puedan acudir a tribunales a fin de tutelar sus derechos en relación al tratamiento de sus datos personales, así, quien se vea afectado puede ejercer la acción de *"habeas data"*, que es aquella procedente cuando el responsable del banco de datos no se pronuncia sobre la solicitud de información, modificación, cancelación o bloqueo en un plazo de dos días hábiles o cuando esta sea denegada. Con la concurrencia de estos requisitos la persona afectada puede recurrir al tribunal del domicilio del responsable del registro o banco de datos. El tribunal deberá dar curso a la solicitud a través de un procedimiento breve y sumario.

De acogerse la reclamación, la sentencia fijará un plazo prudencial para dar cumplimiento a lo resuelto y podrá aplicar una multa de una a diez unidades tributarias mensuales o de diez a

[234] El señalado artículo disponía: "La Constitución asegura a todas las personas, 4° "El respeto y protección a la vida privada y a la honra de la persona y su familia".

cincuenta Unidades Tributarias Mensuales[235], si los datos eran relativos a obligaciones de carácter económico, financiero, bancario o comercial[236].

Este procedimiento ha resultado engorroso y poco efectivo, por cuanto requiere la asesoría letrada, es decir patrocinio de abogado, sumado al bajo valor de la multa que deben pagar los infractores, que en la práctica se traduce en que el incumplimiento a las normas señaladas genera un pago pecuniario que resulta irrisorio para la envergadura de las entidades responsables del registro de datos.

Similar procedimiento también ocurre en el caso español, en el sentido de la regulación tanto constitucional como legal que tiene la protección de datos como derecho fundamental. La CE, como ya se ha analizado, aborda la protección de datos en el artículo 18 apartado cuatro, para luego concretizar dicha regulación, eso sí con mucho mayor densidad y especificidad que la legislación chilena, con la ley orgánica 3/2018 sobre Protección de Datos Personales y Garantía de los Derechos Digitales, que en su artículo 27 se refiere al tratamiento de datos relativos a infracciones y sanciones administrativas, y luego entre los artículos 63 a 69 aborda los procedimientos en caso de posible vulneración de la normativa de protección de datos, así como entre los artículos 70 al 78, el régimen de sanciones.

Institucionales – Autoridad de Control

Finalmente, el otro grupo para tutelar estos derechos son las denominadas garantías institucionales, en los que el ordenamiento jurídico crea órganos autónomos e independientes, o también denominadas Autoridades de Control, para velar y promover los derechos y las libertades fundamentales, en este caso la protección de datos personales. Institución inexistente en el sistema chileno y que representa una de las mayores debilidades para la promoción, regulación y control de la protección de datos personales, cuya contrapartida, en el caso español, es la Agencia de Protección de Datos Personales.

En este capítulo se abordarán como mecanismos de tutela, el derecho para presentar reclamaciones ante la respectiva autoridad de control, previstos en el RGPD, y la vía jurisdiccional o la tutela judicial efectiva, analizando principalmente la jurisprudencia del Tribunal de Justicia de la Unión Europea TJUE, desde la entrada en vigor del Reglamento General de Protección de Datos 679/2016, el 25 de mayo del año 2018.

[235] La Unidad Tributaria Mensual (UTM): Unidad definida en Chile que corresponde a un monto de dinero expresado en pesos y determinado por ley, el cual se actualiza en forma permanente por el Índice de Precios al Consumidor (IPC) y se utiliza como medida tributaria. 1 UTM equivale a poco menos de 58,29 euros; 10 UTM equivalen a 583 euros y 50 UTM equivalen a 2.915 euros, calculados al 9 de Noviembre de 2021.

[236] Violler, P. (2017). *"El estado de la protección de datos personales en Chile"*, Santiago, Derechos Digitales, p.27.

La reclamación ante la autoridad de control y la tutela judicial efectiva en el contexto europeo

El derecho de reclamación ante una Autoridad de Control

La Carta de los Derechos Fundamentales de la Unión Europea, CDFUE[237], consagra en el punto 3 del artículo 8, a propósito de la protección de datos de carácter personal que: "El respeto de estas normas estará sujeto al control de una autoridad independiente".

Esta disposición hay que entenderla en armonía con otro precepto de la Carta, el artículo 47 relativo al derecho a la tutela judicial efectiva y a un juez imparcial. Señala este artículo:

> *"Toda persona cuyos derechos y libertades garantizados por el Derecho de la Unión hayan sido violados tiene derecho a la tutela judicial efectiva respetando las condiciones establecidas en el presente artículo.*
> *Toda persona tiene derecho a que su causa sea oída equitativa y públicamente y dentro de un plazo razonable por un juez independiente e imparcial, establecido previamente por la ley. Toda persona podrá hacerse aconsejar, defender y representar.*
> *Se prestará asistencia jurídica gratuita a quienes no dispongan de recursos suficientes siempre y cuando dicha asistencia sea necesaria para garantizar la efectividad del acceso a la justicia".*

A su vez, esta norma debe entenderse en correspondencia con el Convenio Europeo de Derechos Humanos CEDH, específicamente con los artículos 6 y 13. En efecto, el primer párrafo del señalado artículo 47, se relaciona con el artículo 13 del Convenio, que dispone:

> *"Toda persona cuyos derechos y libertades reconocidos en el presente Convenio hayan sido violados tiene derecho a la concesión de un recurso efectivo ante una instancia nacional, incluso cuando la violación haya sido cometida por personas que actúen en el ejercicio de sus funciones oficiales."*

Según el Tribunal de Justicia de la Unión Europea TJUE, este principio general del Derecho de la Unión también se aplica a los Estados miembros cuando estos aplican el Derecho de la Unión[238]. La inclusión de esta jurisprudencia en la Carta no tiene por objeto modificar el sistema de control jurisdiccional establecido en los Tratados ni tampoco alterar las normas relativas a la admisibilidad de los recursos interpuestos directamente ante dicho tribunal.

La Convención Europea ha examinado el sistema de control jurisdiccional de la Unión, incluidas las normas relativas a la admisibilidad, y ha confirmado dicho sistema, si bien se han modificado determinados aspectos, como establecen los artículos 251 a 281 del Tratado de Funcionamiento de la Unión Europea TFUE[239] y, en particular, el párrafo cuarto del artículo

---

[237] Publicada en el Diario Oficial de la Unión Europea C 202, de 7 de junio de 2016. https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:12016P/TXT&from=ES

[238] El Tribunal de Justicia consagró este derecho en su sentencia de 15 de mayo de 1986 como un principio general del Derecho de la Unión (Johnston, asunto 222/84, Rec. 1986, p. 1651; véanse también las sentencias de 15 de octubre de 1987, asunto 222/86, Heylens, Rec. 1987, p. 4097, y de 3 de diciembre de 1992, asunto C-97/91, Borelli, Rec. 1992, p. I-6313).

[239] Artículos que forman parte de la Sección Quinta relativa al El Tribunal de Justicia de la Unión Europea TJUE.

263[240], debe entenderse que el artículo 47, entonces, se aplica respecto de las instituciones de la Unión y de los Estados miembros, cuando aplican el Derecho de la Unión.

El segundo párrafo del artículo 47 de la CDFUE, se relaciona con el apartado 1 del artículo seis del CEDH, que dispone:

> *"Toda persona tiene derecho a que su causa sea oída equitativa, públicamente y dentro de un plazo razonable, por un Tribunal independiente e imparcial, establecido por la Ley, que decidirá los litigios sobre sus derechos y obligaciones de carácter civil o sobre el fundamento de cualquier acusación en materia penal dirigida contra ella. La sentencia debe ser pronunciada públicamente, pero el acceso a la Sala de Audiencia puede ser prohibido a la prensa y al público durante la totalidad o parte del proceso en interés de la moralidad, del orden público o de la seguridad nacional en una sociedad democrática, cuando los intereses de los menores o la protección de la vida privada de las partes en el proceso así lo exijan o en la medida considerada necesaria por el Tribunal, cuando en circunstancias especiales la publicidad pudiera ser perjudicial para los intereses de la justicia."*

Así entonces, en la Unión Europea el derecho a un tribunal no se aplica únicamente a litigios relativos a derechos y obligaciones de carácter civil, por cuanto la Unión se constituye como una comunidad de derecho, tal y como lo estableció el TJUE en el asunto 294/83, "Les Verts con Parlamento Europeo" (sentencia de 23 de abril de 1986, Rec. 1986, p. 1339).

Por último, en relación con el párrafo tercero y final del artículo 47, interesa hacer notar que, de acuerdo con la jurisprudencia del Tribunal Europeo de Derechos Humanos TEDH, debe concederse asistencia jurídica cuando su ausencia pudiera hacer ineficaz la garantía de un recurso efectivo[241]. El Reglamento General de Protección de Datos de la UE no innova sobre el derecho a presentar reclamaciones y a la tutela judicial efectiva, de hecho, esto ya lo consagraba la Directiva 95/46/CE, en este sentido son referencia los casos Weltimmo[242] y Scherems[243], sobre los que debió pronunciarse el TJUE y que influyeron en la actual regulación que en la materia tiene el RGPD.

---

[240] Artículo 263, párrafo 4° del TFUE: "Toda persona física o jurídica podrá interponer recurso, en las condiciones previstas en los párrafos primero y segundo, contra los actos de los que sea destinataria o que la afecten directa e individualmente y contra los actos reglamentarios que la afecten directamente y que no incluyan medidas de ejecución".

[241] Ver sentencia del TEDH de 9.10.1979, Airey, Serie A, Volumen 32, p. 11.

[242] Sentencia de la 3° Sala del TJUE de 1° de octubre de 2015, asunto C-230/14. Ver en: http://curia.europa.eu/juris/document/document.jsf?.text=&docid=168944&pageIndex=0&doclang=ES&mode=Ist&dir=&occ=first&part=1&cid=976896.

[243] Sentencia del TJUE, Gran Sala, de 6 de octubre de 2015, asunto C-362/14, Ver en: http://curia.europa.eu/juris/document/document.jsf?text=&docid=169195&pageIndex=0&doclang=ES&mode=Ist&dir=&occ=firts&part=1&cid=976005. Esta sentencia, muestra uno de los momentos más álgidos en las relaciones entre la UE y EE. UU en materia de protección de datos, por cuanto puntualiza la necesidad de contar con estándares comunes de protección entre los países de la Unión y EE. UU. Este fallo declaró invalido, después de 15 años de funcionamiento, el denominado acuerdo de "Puerto Seguro", en virtud del cual la Comisión Europea respaldaba y autorizaba la transferencia de datos personales entre empresas de la UE y los Estados Unidos, por considerar que este acuerdo cumplía con los adecuados estándares de protección de datos y que con este fallo quedan sin efecto declarando invalida la Decisión 2000/520/CE de la Comisión.

En el caso Weltimmo y sobre la aplicación del derecho de la UE respecto de instituciones de tratamientos de datos situadas en el territorio de un Estado miembro y la determinación del derecho aplicable y de la autoridad de control competente, resulta ilustrativa la parte resolutiva de esta sentencia, que señala: "En virtud de todo lo expuesto, el Tribunal de Justicia (Sala Tercera) declara: 1)El artículo 4, apartado 1, letra a), de la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, debe interpretarse en el sentido de que permite aplicar la legislación relativa a la protección de los datos personales de un Estado miembro distinto de aquel en el que está registrado el responsable del tratamiento de esos datos, siempre que éste ejerza, mediante una instalación estable en el territorio de dicho Estado miembro, una actividad efectiva y real, aun mínima, en cuyo marco se realice el referido tratamiento. Para determinar si así ocurre, en circunstancias como las controvertidas en el litigio principal, el órgano jurisdiccional remitente puede tener en cuenta, por un lado, que la actividad del responsable de dicho tratamiento, en cuyo marco éste tiene lugar, consiste en la gestión de sitios de Internet de anuncios de inmuebles situados en el territorio de dicho Estado miembro y redactados en la lengua de ese Estado y que, en consecuencia, se dirige principalmente, incluso íntegramente, a dicho Estado miembro y, por otro lado, que ese responsable dispone de un representante en el referido Estado miembro que se encarga de cobrar los créditos resultantes de dicha actividad y de representarlo en los procedimientos administrativo y judicial relativos al tratamiento de los datos en cuestión. En cambio, es irrelevante el tema de la nacionalidad de las personas afectadas por dicho tratamiento de datos. 2) En el supuesto de que la autoridad de control de un Estado miembro que entiende de unas denuncias, de conformidad con el artículo 28, apartado 4, de la Directiva 95/46, llegue a la conclusión de que el Derecho aplicable al tratamiento de los datos personales de que se trata no es el Derecho de ese Estado miembro, sino el de otro Estado miembro, el artículo 28, apartados 1, 3 y 6, de esa misma Directiva debe interpretarse en el sentido de que dicha autoridad de control sólo podría ejercer en el territorio de su propio Estado miembro las facultades efectivas de intervención que se le han conferido conforme al artículo 28, apartado 3, de la citada Directiva. Por lo tanto, no puede imponer sanciones basándose en el Derecho de ese Estado miembro al responsable del tratamiento de tales datos que no está establecido en dicho territorio, sino que, con arreglo al artículo 28, apartado 6, de la misma Directiva, debe instar la intervención de la autoridad de control dependiente del Estado miembro cuyo Derecho es aplicable. 3) La Directiva 95/46 debe interpretarse en el sentido de que el concepto de "adatfeldolgozás" (procesamiento de datos), utilizado en la versión húngara de esta Directiva, en particular en sus artículos 4, apartado 1, letra a), y 28, apartado 6, tiene el mismo sentido que el término "adatkezelés" (tratamiento de datos).

Respecto del caso Scherems, la sentencia muestra uno de los momentos más álgidos en las relaciones entre la UE y EE. UU en materia de protección de datos, por cuanto puntualiza la necesidad de contar con estándares comunes de protección entre los países de la Unión Europea y EE. UU. Este fallo declaró inválido, después de 15 años de funcionamiento, el denominado acuerdo de "Puerto Seguro", en virtud del cual la Comisión Europea respaldaba y autorizaba la transferencia de datos personales entre empresas de la UE y los Estados Unidos, por considerar que este acuerdo cumplía con los adecuados estándares de protección de datos y que con este fallo quedan sin efecto, declarando inválida la Decisión 2000/520/CE de la Comisión.

Como se señaló, la Directiva 95/46/CE ya consagraba en su artículo 28, apartado cuatro[244], que la autoridad de control en materia de protección de datos debía estar dotada de potestades o poderes que le faculten para recibir reclamaciones de los titulares o interesados en la afectación de sus derechos de protección de datos de carácter personal. Este derecho es entonces un derecho principal o toral, en el que las autoridades de control tienen un rol fundamental en orden a garantizar adecuadamente su ejercicio. Sobre este punto, la Agencia de los Derechos Fundamentales de la Unión Europea ha señalado que "Conforme el artículo 28(4)(1) de la Directiva de Protección de Datos las autoridades de control deben estar dotadas de poderes para escuchar reclamaciones presentadas por cualquier persona, o por una asociación que represente a dicha persona, en relación con la protección de sus derechos y libertades sobre el tratamiento de sus datos personales e informar a la persona de que se trata el resultado de la reclamación"[245].

El derecho a presentar reclamaciones ante la autoridad de control

Este derecho (así como el derecho a tutela judicial efectiva), está consagrado en el RGPD, concretamente en el considerando 141, que señala:

> "*Todo interesado debe tener derecho a presentar una reclamación ante una autoridad de control única, en particular en el Estado miembro de su residencia habitual, y derecho a la tutela judicial efectiva de conformidad con el artículo 47 de la Carta si considera que se vulneran sus derechos con arreglo al presente Reglamento o en caso de que la autoridad de control no responda a una reclamación, rechace o desestime total o parcialmente una reclamación o no actúe cuando sea necesario para proteger los derechos del interesado. La investigación a raíz de una reclamación debe llevarse a cabo, bajo control judicial, si procede en el caso concreto. La autoridad de control debe informar al interesado de la evolución y el resultado de la reclamación en un plazo razonable. Si el asunto requiere una mayor investigación o coordinación con otra autoridad de control, se debe facilitar información intermedia al interesado. Para facilitar la presentación de reclamaciones, cada autoridad de control debe adoptar medidas como el suministro de un formulario de reclamaciones, que pueda cumplimentarse también por medios electrónicos, sin excluir otros medios de comunicación".*

De igual forma se reconoce este derecho en el apartado 1 del artículo 77 del señalado Reglamento, el cual dispone:

---

[244] "Toda autoridad de control entenderá de las solicitudes que cualquier persona, o cualquier asociación que la represente, le presente en relación con la protección de sus derechos y libertades respecto del tratamiento de datos personales. Esa persona será informada del curso dado a su solicitud.

Toda autoridad de control entenderá, en particular, de las solicitudes de verificación de la licitud de un tratamiento que le presente cualquier persona cuando sean de aplicación las disposiciones nacionales tomadas en virtud del artículo 13 de la presente Directiva. Dicha persona será informada en todos los casos de que ha tenido lugar una verificación".

[245] Agencia de los Derechos Fundamentales de la Unión Europea, *Data Protection in the European Union: the role of National Data protection Autohorities*, Oficina de Publicaciones de la Unión Europea, Luxemburgo, 2010, p.24.

> *"Sin perjuicio de cualquier otro recurso administrativo o acción judicial, todo interesado tendrá derecho a presentar una reclamación ante una autoridad de control, en particular en el Estado miembro en el que tenga su residencia habitual, lugar de trabajo o lugar de la supuesta infracción, si considera que el tratamiento de datos personales que le conciernen infringe el presente Reglamento"*.

De lo expuesto, es posible concluir que todo titular del derecho de datos de carácter personal o interesado tiene derecho a recurrir ante una autoridad de control, especialmente en el Estado miembro en que tenga su residencia habitual, en que trabaje o en el territorio del lugar donde se haya producido la supuesta infracción al Reglamento (y lo mismo aplica respecto de la infracción a la normativa nacional respectiva[246]). Así entonces, podrá entablar una acción judicial o recurso ante las autoridades jurisdiccionales de los Estados miembros, de conformidad a su respectiva legislación. En definitiva, el interesado está facultado o tiene derecho a:

a) Interponer recursos administrativos ante la autoridad de control[247].
b) Interponer recursos judiciales ante el órgano jurisdiccional competente.
c) Recurrir a mecanismos de resolución extrajudicial de conflictos.

Este derecho a la reclamación ante la autoridad de control, también está previsto como las normas corporativas vinculantes[248] a la que hace referencia la parte final de la letra e) del apartado 2 del artículo 47 del RGPD, que establece: "…el derecho a presentar una reclamación ante la autoridad de control competente y ante los tribunales competentes de los Estados miembros de conformidad con el artículo 79[249], y el derecho a obtener una reparación, y, cuando proceda, una indemnización por violación de las normas corporativas vinculantes".

En definitiva, este derecho cuyo titular es el interesado, supone que la autoridad de control debe analizar cualquier solicitud que se le presente relativa al tratamiento de datos personales, tal como incluso lo ha dispuesto el TJUE a propósito del caso Schrems, en la parte final del apartado 33 de la sentencia al señalar: "… el asunto principal se tuviera que resolver con fundamento exclusivo en el Derecho irlandés, se debería apreciar que, dada la existencia de serias dudas de que Estados Unidos garantice un nivel adecuado de protección de los datos personales, el comisario habría debido llevar a cabo una investigación sobre los hechos denunciados por el Sr. Schrems en su reclamación, y que la desestimó indebidamente".

---

[246] En el caso español ante la Agencia Española de Protección de Datos, en el caso chileno, no existe una autoridad de control en la materia.

[247] Puente Escobar, A. (2008), "La Agencia Española de Protección de Datos como garante del derecho fundamental a la protección de datos de carácter personal", *Azpilcueta*, n°20, pp.13-41.

[248] Que están definidas en el N° 20 del artículo 4 del RGPD como: "las políticas de protección de datos personales asumidas por un responsable o encargado del tratamiento establecido en el territorio de un Estado miembro para transferencias o un conjunto de transferencias de datos personales a un responsable o encargado en uno o más países terceros, dentro de un grupo empresarial o una unión de empresas dedicadas a una actividad económica conjunta".

[249] Artículo que se refiere al Derecho a la tutela judicial efectiva contra un responsable o encargado del tratamiento.

Cada autoridad de control, como una forma de facilitar la presentación de reclamaciones, debe poner a disposición de los interesados un formulario de reclamaciones que pueda rellenarse también por medios electrónicos, pudiendo utilizar otros medios de comunicación.

Del apartado 2 del artículo 77 del RGPD se desprende que la autoridad de control ante la cual se haya presentado la reclamación informará al reclamante sobre el curso y resultado de su presentación, así como de la posibilidad de acceder a la tutela judicial.

Reclamación, Transparencia e Información

Otro aspecto a considerar sobre el derecho a reclamación es su relación con otros derechos que están establecidos en el Reglamento, como es el caso del derecho a la transparencia y el derecho de información al interesado, así, a propósito del derecho de transparencia, el apartado 4 del artículo 12 del RGPD dispone que;

> *"Si el responsable del tratamiento no da curso a la solicitud del interesado, le informará sin dilación, y a más tardar transcurrido un mes de la recepción de la solicitud, de las razones de su no actuación y de la posibilidad de presentar una reclamación ante una autoridad de control y de ejercitar acciones judiciales"*.

De igual forma el artículo 13 del Reglamento sobre el derecho de información al interesado, establece en el apartado 2 letra d) "el derecho a presentar una reclamación ante una autoridad de control", en idénticos términos lo dispone el artículo 15 sobre el derecho de acceso en el apartado 1 letra f.

Es decir, como se puede apreciar, el responsable del tratamiento de datos de carácter personal tiene el deber de informar el derecho a presentar reclamaciones ante la respectiva autoridad que tiene el titular del derecho de protección de datos personales o interesado, tal como se desprende de la normativa reglamentaria precedentemente descrita.

Sobre la competencia[250], funciones y poderes de la autoridad de control para hacerse cargo de las reclamaciones presentadas se refieren los artículos 56, 57 y 58 del Reglamento y se abordarán en extenso en los siguientes capítulos de la presente investigación. Por ahora es procedente señalar que el apartado 2 del artículo 56 en lo que a esto se refiere señala:

> *"…cada autoridad de control será competente para tratar una reclamación que le sea presentada o una posible infracción del presente Reglamento, en caso de que se refiera únicamente a un establecimiento situado en su Estado miembro o únicamente afecte de manera sustancial a interesados en su Estado miembro"*.

Sobre este punto resulta relevante considerar el caso Weltimmo, donde el TJUE, resolviendo sobre la medida prejudicial que se formuló, debió pronunciarse sobre la autoridad de control competente en caso de vulneración del derecho a la protección de datos de un Estado miembro, por un responsable del tratamiento de datos establecido formalmente en otro Estado miembro;

[250] Conviene señalara aquí, que la competencia de los órganos de la administración del Estado o servicios públicos en el ordenamiento jurídico chileno es un concepto jurídico indeterminado, esto es, ni la Constitución ni la ley han definido el término competencia, el que se entiende por la doctrina como la habilitación, es decir una autorización y a la vez facultad para que un órgano de la administración se haga cargo de ciertas y determinadas funciones, en un determinado territorio o ámbito espacial.

en efecto, en el punto 57 de la sentencia se establece: "Así pues, cuando una autoridad de control entienda de una denuncia, de conformidad con el artículo 28, apartado 4, de la Directiva 95/46, puede ejercer sus facultades de investigación sea cual sea el Derecho aplicable e incluso antes de saber cuál es el Derecho nacional aplicable al tratamiento de que se trata. Sin embargo, si llega a la conclusión de que es aplicable el Derecho de otro Estado miembro, no puede imponer sanciones fuera del territorio de su propio Estado miembro. En tal situación, le corresponde instar, en ejecución de la obligación de cooperación que se establece en el artículo 28, apartado 6, de la citada Directiva, a la autoridad de control de ese otro Estado miembro a declarar una eventual infracción de ese Derecho y a imponer sanciones si éste lo permite, basándose, en su caso, en la información que ella le haya remitido". A su vez en la parte resolutiva (apartado 2 del fallo) dispone; "En el supuesto de que la autoridad de control de un Estado miembro que entiende de unas denuncias, de conformidad con el artículo 28, apartado 4, de la Directiva 95/46, llegue a la conclusión de que el Derecho aplicable al tratamiento de los datos personales de que se trata no es el Derecho de ese Estado miembro, sino el de otro Estado miembro, el artículo 28, apartados 1, 3 y 6, de esa misma Directiva debe interpretarse en el sentido de que dicha autoridad de control sólo podría ejercer en el territorio de su propio Estado miembro las facultades efectivas de intervención que se le han conferido conforme al artículo 28, apartado 3, de la citada Directiva".

Sobre la competencia tanto de la autoridad de control principal como de otras autoridades de control, hay que tener presente el principio de cooperación que se deriva del artículo 60 del RGPD, que precisamente se refiere a la cooperación entre la autoridad de control principal y las demás autoridades de control interesadas. En efecto, de los apartados 7[251], 8[252] y 9[253] del señalado artículo, es posible desprender el trabajo colaborativo que les corresponde realizar, debiendo la autoridad de control ante la cual se haya presentado la reclamación, informar de la decisión que se adopte al interesado o reclamante. Y de igual forma, cuando se rechace una reclamación, la autoridad de control ante la cual se haya presentado dicha reclamación será la que decidirá, notificando al reclamante, e informará de ello al responsable del tratamiento.

[251] "La autoridad de control principal adoptará y notificará la decisión al establecimiento principal o al establecimiento único del responsable o el encargado del tratamiento, según proceda, e informará de la decisión a las autoridades de control interesadas y al Comité, incluyendo un resumen de los hechos pertinentes y la motivación. La autoridad de control ante la que se haya presentado una reclamación informará de la decisión al reclamante".

[252] "No obstante lo dispuesto en el apartado 7, cuando se desestime o rechace una reclamación, la autoridad de control ante la que se haya presentado adoptará la decisión, la notificará al reclamante e informará de ello al responsable del tratamiento".

[253] "En caso de que la autoridad de control principal y las autoridades de control interesadas acuerden desestimar o rechazar determinadas partes de una reclamación y atender otras partes de ella, se adoptará una decisión separada para cada una de esas partes del asunto. La autoridad de control principal adoptará la decisión respecto de la parte referida a acciones en relación con el responsable del tratamiento, la notificará al establecimiento principal o al único establecimiento del responsable o del encargado en el territorio de su Estado miembro, e informará de ello al reclamante, mientras que la autoridad de control del reclamante adoptará la decisión respecto de la parte relativa a la desestimación o rechazo de dicha reclamación, la notificará a dicho reclamante e informará de ello al responsable o al encargado".

Finalmente, en la eventualidad que la autoridad de control principal y las otras autoridades de control intervinientes acuerden rechazar determinadas partes de la reclamación y acoger otras, se adoptará una decisión separada.

Sobre las funciones, el apartado 1 letra f) del artículo 57 indica que a cada autoridad de control en su territorio le corresponde: "tratar las reclamaciones presentadas por un interesado o por un organismo, organización o asociación de conformidad con el artículo 80, e investigar, en la medida oportuna, el motivo de la reclamación e informar al reclamante sobre el curso y el resultado de la investigación en un plazo razonable, en particular si fueran necesarias nuevas investigaciones o una coordinación más estrecha con otra autoridad de control".

El Derecho a la tutela judicial efectiva

Como ya se señaló, la CDFUE en su artículo 47 también reconoce que todo titular de derechos fundamentales, en este caso de protección de datos o interesado, tiene derecho a la tutela judicial efectiva contra una autoridad de control si sus derechos de conformidad al RGPD son transgredidos o vulnerados, también podrá recurrirse contra una decisión jurídicamente vinculante que le concierna que haya adoptado una autoridad de control, o también en caso que la autoridad de control competente no responda frente a un requerimiento que se le presente, o rechace o desestime una reclamación total o parcial, o no actúe cuando sea necesario para proteger los derechos del interesado, o no dé curso a una reclamación o no informe al interesado en el plazo de tres meses sobre el curso, o resultado de la reclamación presentada, de conformidad al artículo 77 del Reglamento.

Lo anterior es sin perjuicio de los dispuesto en los apartados 1 y 2 del artículo 78 del RGPD, es decir:

> "*1. Sin perjuicio de cualquier otro recurso administrativo o extrajudicial, toda persona física o jurídica tendrá derecho a la tutela judicial efectiva contra una decisión jurídicamente vinculante de una autoridad de control que le concierna; y 2. Sin perjuicio de cualquier otro recurso administrativo o extrajudicial, todo interesado tendrá derecho a la tutela judicial efectiva en caso de que la autoridad de control que sea competente en virtud de los artículos 55 y 56 no dé curso a una reclamación o no informe al interesado en el plazo de tres meses sobre el curso o el resultado de la reclamación presentada en virtud del artículo 77".*

Así entonces podrá impugnar o recurrir:

a) Una decisión jurídicamente vinculante de una autoridad de control que le concierna.
b) Cuando la autoridad de control competente no dé curso a una reclamación o no informe al interesado en el plazo de tres meses sobre el curso o el resultado de la reclamación presentada ante una autoridad de control.

En cualquier caso, las acciones contra una autoridad de control deberán ejercerse ante los tribunales del Estado miembro en que está establecida dicha autoridad de control y cuando se ejerciten acciones contra una decisión de una autoridad de control que haya sido precedida de un dictamen o de una decisión del Comité en el contexto del mecanismo de coherencia, la

autoridad de control remitirá al tribunal dicho dictamen o decisión, según se desprende de los apartados 3[254] y 4[255] del artículo 78 del Reglamento.

En relación a la tutela judicial efectiva contra un responsable o encargado del tratamiento de datos, el apartado 1 del artículo 79 del Reglamento dispone:

> "*Sin perjuicio de los recursos administrativos o extrajudiciales disponibles, incluido el derecho a presentar una reclamación ante una autoridad de control en virtud del artículo 77, todo interesado tendrá derecho a la tutela judicial efectiva cuando considere que sus derechos en virtud del presente Reglamento han sido vulnerados como consecuencia de un tratamiento de sus datos personales"*.

Estas acciones deberán interponerse ante los tribunales del Estado miembro en que el responsable o encargado tenga su establecimiento. Aun cuando alternativamente esas acciones puedan ejercerse ante los tribunales del Estado miembro en que el interesado tenga su residencia habitual a no ser que el responsable o encargado sea una autoridad pública del Estado miembro que actúe en el ejercicio de sus potestades públicas. A esto se refiere el considerando 145 del RGPD al señalar:

> "*Por lo que respecta a las acciones contra los responsables o encargados del tratamiento, el reclamante debe tener la opción de ejercitarlas ante los tribunales de los Estados miembros en los que el responsable o el encargado tenga un establecimiento o resida el interesado, a menos que el responsable sea una autoridad pública de un Estado miembro que actúe en el ejercicio de poderes públicos"*.

Este derecho a tutela o recurso judicial está relacionado también con la denominada ventanilla única[256], que fue ampliamente abordada durante la tramitación del RGPD[257]. En efecto, lo

---

[254] "Las acciones contra una autoridad de control deberán ejercitarse ante los tribunales del Estado miembro en que esté establecida la autoridad de control".

[255] "Cuando se ejerciten acciones contra una decisión de una autoridad de control que haya sido precedida de un dictamen o una decisión del Comité en el marco del mecanismo de coherencia, la autoridad de control remitirá al tribunal dicho dictamen o decisión".

[256] En ingles "one, stop, shop."

[257] Ver: Hustinx, P. (2013), *"EU Data Protection Law: The Review of Directive 95/46/CE and the Proposed General Data Protection Regulation"*, del cual se desprende traducido al español: "En este contexto, el solo hecho de que los Tribunales de un Estado miembro distinto al del país de residencia de un ciudadano deban ser llamados, no priva por sí mismo a los ciudadanos de la protección judicial efectiva. En virtud de la actual Directiva 95/46/CE, también es posible que los ciudadanos que deseen presentar una reclamación sobre el tratamiento de datos personales por parte de una empresa que operan en numerosos Estados miembros deben dirigirse a una ADP especifica y, si desean recurrir sus decisiones, deben continuar con el litigio en ese mismo Estado miembro. Hasta el momento no ha habido ninguna razón para cuestionar en virtud de la Carta esa función del sistema actual. El principio de ventanilla única propuesto también es criticado por crear obstáculos excesivos para los ciudadanos que buscan recursos judiciales debido a la distancia geográfica, la falta de familiaridad con un sistema legal extranjero, la necesidad de iniciar y llevar a cabo un procedimiento en una lengua extranjera, o los costes de tal procedimiento". En E.J. Numan et al. (ed.) (2010), "*Massificatie in het privaatrecht*" , at 77-91, and P. Hustinx, (2013), *"EU Data Protection Law - Current State and Future Perspectives*", speech at High Level Conference: 'Ethical Dimensions of Data Protection and Privacy', Centre for Ethics, University of Tartu / Data Protection Inspectorate, Tallinn, Estonia, 9 January 2013, available at https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Speeches/2013/13-01-09_Speech_Tallinn_EN.pdf (last accessed 31 May 2014). The author is grateful for comments made on a draft version by C. Docksey.

prioritario es asegurar el derecho a impugnación del interesado, incluso cuando hubiera presentado un recurso en un Estado miembro diferente al de su residencia, tratándose de una reclamación contra el tratamiento de datos de una entidad u organización que funciona en varios Estados miembros, por lo que el interesado tendrá derecho a recurrir contra la decisión de la autoridad de control en el mismo Estado miembro en que presentó su reclamación, tal como ocurrió en el caso Schrems, donde el reclamante, un ciudadano austríaco residente en Irlanda, presentó su reclamación ante la autoridad de control irlandesa, impugnando o recurriendo posteriormente la decisión ante los tribunales de dicho Estado miembro.

En definitiva, la tutela judicial efectiva evolucionó desde sus orígenes en que era concebida como un derecho accesorio o complementario a otros, a ser un derecho fundamental reconocido en el artículo 47 de la CDFUE, vinculado al derecho de protección de datos de carácter personal, regulado en el RGPD 2016/679, que ha ampliado el contenido y alcance de dicha tutela, en relación a la regulación que estaba prevista en la Directiva 95/46/CE, donde la influencia de la jurisprudencia del TJUE ha sido fundamental.

La jurisprudencia del Tribunal de Justicia de la Unión Europea (TJUE) sobre protección de datos

El desarrollo que la protección de datos de carácter personal ha tenido en el ámbito europeo, está también relacionada con los abundantes fallos que este órgano jurisdiccional supra estatal ha emitido en el último tiempo. Lo que fundamentalmente tiene a lo menos dos antecedentes; primero, el vertiginoso incremento de las tecnologías de la información y el desarrollo del *Big Data*, que ha permitido no solo la multiplicación de información y datos de las personas, sino que también su creciente almacenamiento a gran escala. Y, en segundo lugar, la competencia especifica que para la regulación del derecho fundamental de la protección de datos de carácter personal tiene en el espacio de la Unión Europea, derivada de la Carta de Derechos Fundamentales de la Unión Europea CDFUE y por consiguiente del Tribunal Europeo de Derechos Humanos TEDH.

En términos similares a lo que ocurre con la regulación normativa, la jurisprudencia ha evolucionado en el reconocimiento y tutela de la protección de datos de carácter personal, y en este sentido, el aporte del TJUE a través de la interpretación y resolución de las contiendas sometidas a su conocimiento ha sido fundamental, pudiendo distinguirse sus aportes jurisprudenciales en materias relacionadas con la divulgación de datos personales, la independencia de las autoridades de control en protección de datos, definición y alcance del término datos personales y delimitación de los derechos del interesado por mencionar algunas.

Como es lógico, la mayor cantidad de fallos que este órgano jurisdiccional ha emitido en el último tiempo tienen como marco regulatorio la Directiva 95/46/CE vigente hasta el año 2018, por lo que la revisión que a continuación se realizará de la jurisprudencia del TJUE considera los asuntos concluidos en el repertorio de jurisprudencia de ese tribunal en el periodo comprendido entre el 25 de mayo de 2018, fecha en la que entra en vigor el Reglamento General de Protección de Datos RGPD 2016/679, y mayo de 2020. Sin perjuicio de las

referencias que las sentencias estudiadas hagan a la anterior Directiva, teniendo en cuenta las fechas en que los requerimientos fueron presentados ante dicha instancia jurisdiccional[258].

En efecto, de la señalada búsqueda se registran once asuntos, de los que se hará una descripción y análisis en orden cronológico, de diez de ellos, que son los que están accesibles al público[259].

Sentencia T-452/17 – TL/SEPD, del 28 de junio de 2018

El primer fallo es un Auto del Tribunal General (Sala Sexta)**,** del 28 de junio de 2018, individualizado como T-452/17 – TL/SEPD, que tuvo como objeto la presentación de un recurso basado en el artículo 263 TFUE[260] por el que se solicita la anulación de la decisión del Supervisor Europeo de Protección de Datos (SEPD) de 16 de mayo de 2017, por la que no se admitió a tramitación la reclamación que tenía por objeto, por un lado, que el SEPD procediera a un nuevo análisis de su competencia en relación con la difusión en Internet del nombre de una parte de un procedimiento por el Tribunal de Justicia de la Unión Europea y, por otro lado, que se ordenara la anonimización de la sentencia. Finalmente, el fallo desestima el recurso por inadmisibilidad manifiesta.

---

258 Recapitulación de los criterios seleccionados: Materia = "Protección de datos "Situación de los asuntos = "Asuntos concluidos "Período o fecha = "Fecha de pronunciamiento"; Período= "de 25/05/2018 al 05/05/2020".Ver:http://curia.europa.eu/juris/liste.jsf?oqp=&for=&mat=PDON%252Cor&jge=&td=%3BALL&jur=C%2CT%2CF&etat=clot&page=1&dates=%2524type%253Dpro%2524mode%253DfromTo%2524from%253D2018.05.25%2524to%253D2020.05.05&pcs=Oor&lg=&pro=&nat=or&cit=none%252CC%252CCJ%252CR%252C2008E%252C%252C%252C%252C%252C%252C%252C%252C%252C%252Ctrue%252Cfalse%252Cfalse&language=es&avg=&cid=6353991 consulta realizada el 05 de mayo de 2020.

259 La sentencia C-687/18 - *Associated Newspapers,* Auto del Tribunal de Justicia (Gran Sala) de 4 de noviembre de 2019, SY contra *Associated Newspapers Ltd*., no registra información no está disponible.

260 Artículo 263 del TFUE: "El Tribunal de Justicia de la Unión Europea controlará la legalidad de los actos legislativos, de los actos del Consejo, de la Comisión y del Banco Central Europeo que no sean recomendaciones o dictámenes, y de los actos del Parlamento Europeo y del Consejo Europeo destinados a producir efectos jurídicos frente a terceros. Controlará también la legalidad de los actos de los órganos u organismos de la Unión destinados a producir efectos jurídicos frente a terceros.

A tal fin, el Tribunal de Justicia de la Unión Europea será competente para pronunciarse sobre los recursos por incompetencia, vicios sustanciales de forma, violación de los Tratados o de cualquier norma jurídica relativa a su ejecución, o desviación de poder, interpuestos por un Estado miembro, el Parlamento Europeo, el Consejo o la Comisión.

El Tribunal de Justicia de la Unión Europea será competente en las mismas condiciones para pronunciarse sobre los recursos interpuestos por el Tribunal de Cuentas, por el Banco Central Europeo y por el Comité de las Regiones con el fin de salvaguardar prerrogativas de éstos.

Toda persona física o jurídica podrá interponer recurso, en las condiciones previstas en los párrafos primero y segundo, contra los actos de los que sea destinataria o que la afecten directa e individualmente y contra los actos reglamentarios que la afecten directamente y que no incluyan medidas de ejecución.

Los actos por los que se crean los órganos y organismos de la Unión podrán prever condiciones y procedimientos específicos para los recursos presentados por personas físicas o jurídicas contra actos de dichos órganos u organismos destinados a producir efectos jurídicos frente a ellos.

Los recursos previstos en el presente artículo deberán interponerse en el plazo de dos meses a partir, según los casos, de la publicación del acto, de su notificación al recurrente o, a falta de ello, desde el día en que éste haya tenido conocimiento del mismo".

Sentencia C-207/16 – Ministerio Fiscal, de 2 de octubre de 2018

El segundo fallo es el de una Sentencia del TJUE (Gran Sala) de 2 de octubre de 2018, individualizada con el C-207/16 – Ministerio Fiscal, que tenía por objeto la interpretación del artículo 15, apartado 1, de la Directiva 2002/58/CE, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas (Directiva sobre la privacidad y las comunicaciones electrónicas), en relación con los artículos 7 y 8 de la Carta de los Derechos Fundamentales de la Unión Europea CDFUE.

Este requerimiento se presentó en el marco de un recurso interpuesto por el Ministerio Fiscal contra la resolución del Juzgado de Instrucción N° 3 de Tarragona o juez instructor, relativa a la denegación de acceso de la Policía Judicial a datos personales almacenados por proveedores de servicios de comunicaciones electrónicas. En efecto, según se desprende de la sentencia en análisis los hechos pueden resumirse así: El Sr. Hernández Sierra presentó una denuncia ante la Policía por un robo con violencia, cometido el 16 de febrero de 2015, durante el cual resultó herido y en el que además le sustrajeron su cartera y su teléfono móvil.

El 27 de febrero de 2015, la Policía Judicial presentó un oficio ante el juez instructor solicitando que se ordenase a diversos proveedores de servicios de comunicaciones electrónicas la transmisión de los números de teléfono activados, entre el 16 de febrero y el 27 de febrero de 2015, con el código relativo a la identidad internacional del equipo móvil o código IMEI del teléfono sustraído, así como los datos personales o de filiación de los titulares o usuarios de los números de teléfono correspondientes a las tarjetas SIM activadas con dicho código, como su nombre, apellidos y dirección.

Mediante auto de 5 de mayo de 2015, el juez instructor denegó la diligencia solicitada por cuanto consideró que no era idónea para identificar a los autores del delito y porque la Ley 25/2007 limitaba la cesión de los datos conservados por las operadoras de telefonía a los delitos graves que según el Código Penal español son los sancionados con una pena de prisión superior a cinco años, estimando dicho juez, que los hechos investigados no eran constitutivos de delito grave. El Ministerio Fiscal interpuso recurso de apelación contra dicho auto ante el tribunal remitente.

Entre otras consideraciones, el tribunal remitente afirma que en diversas sentencias se ha reconocido que la conservación y cesión de datos de tráfico constituyen injerencias graves a los derechos garantizados por los artículos 7 y 8 de la CDFUE e identificó entre los criterios de apreciación el principio de proporcionalidad, que en este caso deriva en la gravedad de los delitos que justifican la conservación de estos datos y el acceso a ellos para la investigación de un delito, gravedad de los ilícitos que en el caso en estudio no se configuraría.

En estas circunstancias, la Audiencia Provincial de Tarragona decidió suspender el procedimiento y plantear al Tribunal de Justicia de la UE en lo sustancial la siguiente cuestión prejudicial: Es la gravedad de los delitos el criterio que justifica la injerencia en los derechos fundamentales reconocidos en los artículos 7 y 8 de la Carta, una causal que puede identificarse únicamente considerando la pena que pueda imponerse al delito que se investiga o es necesario, además, identificar en la conducta delictiva, particulares niveles de lesividad para bienes jurídicos individuales y/o colectivos.

Para la resolución de este asunto el TJUE, tuvo en consideración las siguientes disposiciones; el artículo 3 de la Directiva 95/46/CE, sobre el ámbito de aplicación de esta, así como los

considerandos 2, 11, 15 y 21 de la Directiva 2002/58 sobre la privacidad y las comunicaciones electrónicas. De igual forma analizó el artículo 1 de la Directiva 2002/58, también referido a su ámbito de aplicación y objetivo, así como el artículo 5 de la Directiva 2002/58, sobre confidencialidad de las comunicaciones. A continuación se trascriben las citadas disposiciones:

> *Artículo 3 de la Directiva 95/46; "Las disposiciones de la presente Directiva se aplicarán al tratamiento total o parcialmente automatizado de datos personales, así como al tratamiento no automatizado de datos personales contenidos o destinados a ser incluidos en un fichero", y luego agrega, "Las disposiciones de la presente Directiva no se aplicarán al tratamiento de datos personales: efectuado en el ejercicio de actividades no comprendidas en el ámbito de aplicación del Derecho comunitario, como las previstas por las disposiciones de los títulos V y VI del Tratado de la Unión Europea y, en cualquier caso, al tratamiento de datos que tenga por objeto la seguridad pública, la defensa, la seguridad del Estado (incluido el bienestar económico del Estado cuando dicho tratamiento esté relacionado con la seguridad del Estado) y las actividades del Estado en materia penal".*
>
> *Considerando 2 de la Directiva 2002/58; "La presente Directiva pretende garantizar el respeto de los derechos fundamentales y observa los principios consagrados, en particular, en la [Carta]. Señaladamente, la presente Directiva pretende garantizar el pleno respeto de los derechos enunciados en los artículos 7 y 8 de [esta]".*
>
> *Considerando 11 de la Directiva 2002/58; Al igual que la Directiva [95/46], la presente Directiva no aborda la protección de los derechos y las libertades fundamentales en relación con las actividades no regidas por el Derecho comunitario. Por lo tanto, no altera el equilibrio actual entre el derecho de las personas a la intimidad y la posibilidad de que disponen los Estados miembros, según se indica en el apartado 1 del artículo 15 de la presente Directiva, de tomar las medidas necesarias para la protección de la seguridad pública, la defensa, la seguridad del Estado (incluido el bienestar económico del Estado cuando las actividades tengan relación con asuntos de seguridad del Estado) y la aplicación del Derecho penal. En consecuencia, la presente Directiva no afecta a la capacidad de los Estados miembros para interceptar legalmente las comunicaciones electrónicas o tomar otras medidas, cuando sea necesario, para cualquiera de estos fines y de conformidad con el Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales, según la interpretación que se hace de este en las sentencias del Tribunal Europeo de Derechos Humanos. Dichas medidas deberán ser necesarias en una sociedad democrática y rigurosamente proporcionales al fin que se pretende alcanzar y deben estar sujetas, además, a salvaguardias adecuadas, de conformidad con el Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales".*
>
> *Considerando 15 de la Directiva 2002/58; "Una comunicación puede incluir cualquier dato relativo a nombres, números o direcciones facilitado por el remitente de una comunicación o el usuario de una conexión para llevar a cabo la comunicación. Los datos de tráfico pueden incluir cualquier conversión de dicha información*

efectuada por la red a través de la cual se transmita la comunicación a efectos de llevar a cabo la transmisión".

Considerando 21 de la Directiva 2002/58; "Deben adoptarse medidas para evitar el acceso no autorizado a las comunicaciones a fin de proteger la confidencialidad de las mismas, incluidos tanto sus contenidos como cualquier dato relacionado con ellas, por medio de las redes públicas de comunicaciones y los servicios de comunicaciones electrónicas disponibles al público. La legislación nacional de algunos Estados miembros prohíbe solamente el acceso intencionado no autorizado a las comunicaciones".

Artículo 1 de la Directiva 2002/58; "1. La presente Directiva establece la armonización de las disposiciones nacionales necesaria para garantizar un nivel equivalente de protección de las libertades y los derechos fundamentales y, en particular, del derecho a la intimidad y la confidencialidad, en lo que respecta al tratamiento de los datos personales en el sector de las comunicaciones electrónicas, así como la libre circulación de tales datos y de los equipos y servicios de comunicaciones electrónicas en la Comunidad; 2. Las disposiciones de la presente Directiva especifican y completan la Directiva [95/46] a los efectos mencionados en el apartado uno. Además, protegen los intereses legítimos de los abonados que sean personas jurídicas; 3. La presente Directiva no se aplicará a las actividades no comprendidas en el ámbito de aplicación del Tratado constitutivo de la Comunidad Europea, como las reguladas por las disposiciones de los títulos V y VI del Tratado de la Unión Europea, ni, en cualquier caso, a las actividades que tengan por objeto la seguridad pública, la defensa, la seguridad del Estado (incluido el bienestar económico del Estado cuando dichas actividades estén relacionadas con la seguridad del mismo) y a las actividades del Estado en materia penal".

Artículo 5 de la Directiva 2002/58; "1. Los Estados miembros garantizarán, a través de la legislación nacional, la confidencialidad de las comunicaciones, y de los datos de tráfico asociados a ellas, realizadas a través de las redes públicas de comunicaciones y de los servicios de comunicaciones electrónicas disponibles al público. En particular, prohibirán la escucha, la grabación, el almacenamiento u otros tipos de intervención o vigilancia de las comunicaciones y los datos de tráfico asociados a ellas por personas distintas de los usuarios, sin el consentimiento de los usuarios interesados, salvo cuando dichas personas estén autorizadas legalmente a hacerlo de conformidad con el apartado 1 del artículo 15..."

Y en lo que más interesa, el artículo 15 de la mencionada Directiva, sobre aplicación de determinadas disposiciones de la Directiva 95/46/CE, el cual establece en su apartado 1: "Los Estados miembros podrán adoptar medidas legales para limitar el alcance de los derechos y las obligaciones que se establecen en los artículos 5 y 6, en los apartados 1 a 4 del artículo 8 y en el artículo 9 de la presente Directiva, cuando tal limitación constituya una medida necesaria proporcionada y apropiada en una sociedad democrática para proteger la seguridad nacional (es decir, la seguridad del Estado), la defensa, la seguridad pública, o la prevención, investigación, descubrimiento y persecución de delitos o la utilización no autorizada del sistema de comunicaciones electrónicas a que se hace referencia en el apartado 1 del artículo

13 de la Directiva 95/46/CE. Para ello, los Estados miembros podrán adoptar, entre otras, medidas legislativas en virtud de las cuales los datos se conserven durante un plazo limitado justificado por los motivos establecidos en el presente apartado. Todas las medidas contempladas en el presente apartado deberán ser conformes con los principios generales del Derecho comunitario, incluidos los mencionados en los apartados 1 y 2 del artículo 6 del Tratado de la Unión Europea".

Es decir, la propia Directiva 2002/58 dispone y reconoce la facultad de los Estados de adoptar medidas legislativas que afecten la confidencialidad de las comunicaciones y el tráfico de datos vinculados a redes públicas de comunicación, que tengan como fundamento la prevención, investigación, descubrimiento y persecución de delitos. Estableciendo eso sí, como condición, el conservar estos datos por un determinado lapso de tiempo.

En su sentencia el TJUE analiza la justificación de una norma nacional, como la controvertida en el litigio principal, que regula el acceso de las autoridades públicas, en este caso la Policía Judicial, a los datos conservados por los proveedores de servicios de comunicaciones electrónicas y, por tanto, establece una excepción al principio de confidencialidad de las comunicaciones electrónicas, como lo dispone la enumeración de los objetivos que figuran en el artículo 15, apartado 1, primera frase, de la Directiva 2002/58, la que debe entenderse tienen carácter exhaustivo, de modo que dicho acceso ha de responder efectiva y estrictamente a uno de ellos. Así entonces, en lo que se refiere al objetivo de la prevención, investigación, descubrimiento y persecución de delitos, procede observar que el tenor del artículo 15, apartado 1, primera frase, de la Directiva 2002/58 no limita este objetivo a la lucha contra los delitos graves, sino que se refiere a los delitos en general.

De los antecedentes analizados, los datos a que se refiere la solicitud de acceso controvertida solo permiten vincular, durante un período determinado, la tarjeta o tarjetas SIM activadas con el teléfono móvil sustraído y los datos personales o de filiación de los titulares de estas tarjetas SIM. Sin un cotejo con los datos relativos a las comunicaciones realizadas con esas tarjetas SIM y de localización, estos datos no permiten conocer la fecha, la hora, la duración o los destinatarios de las comunicaciones efectuadas con las tarjetas SIM en cuestión, ni los lugares en que estas comunicaciones tuvieron lugar, ni la frecuencia de estas con determinadas personas durante un período concreto. Por lo tanto, esos datos no arrojan conclusiones precisas sobre la vida privada de las personas afectadas.

En tales circunstancias, el acceso limitado únicamente a los datos cubiertos por la solicitud controvertida en el litigio no puede calificarse de injerencia grave en los derechos fundamentales de los individuos cuyos datos se ven afectados.

En consecuencia, como se desprende de los apartados 53 a 57 de la sentencia[261], la injerencia que supone el acceso a dichos datos puede estar justificada por el objetivo de prevenir,

[261] "(53) Pues bien, por lo que se refiere al objetivo de la prevención, investigación, descubrimiento y persecución de delitos, procede observar que el tenor del artículo 15, apartado 1, primera frase, de la Directiva 2002/58 no limita este objetivo a la lucha contra los delitos graves, sino que se refiere a los "delitos" en general; (54) A este respecto, es cierto que el Tribunal de Justicia ha declarado que, en materia de prevención, investigación, descubrimiento y persecución de delitos, solo la lucha contra la delincuencia grave puede justificar un acceso a datos personales conservados por los proveedores de servicios de comunicaciones electrónicas que, considerados en su conjunto, permiten extraer conclusiones precisas sobre la vida privada de las personas cuyos datos han sido conservados...; (55) No obstante, el Tribunal de Justicia ha motivado esa interpretación basándose en que el

investigar, descubrir y perseguir delitos en general, al que se refiere el artículo 15, apartado 1, primera frase, de la Directiva 2002/58, sin que sea necesario que dichos delitos estén calificados como graves. En definitiva, según lo dispuesto en el artículo 15, apartado 1, de la Directiva 2002/58, en relación con los artículos 7 y 8 de la CDFUE, el TJUE interpreta que el acceso de las autoridades públicas a los datos que permiten identificar a los titulares de las tarjetas SIM activadas con un teléfono móvil sustraído, como los nombres, los apellidos y, en su caso, las direcciones de dichos titulares, constituye una injerencia en los derechos fundamentales de estos, consagrados en los citados artículos de la Carta, que no presenta una gravedad tal que dicho acceso deba limitarse, en el ámbito de la prevención, investigación, descubrimiento y persecución de delitos, en la lucha contra la delincuencia grave.

Sentencia C-210/16, Wirstschaftsakademie Schleswig-Holstein, de 5 de junio de 2018

El tercer fallo esta individualizado como C- 210/16 – *Wirstschaftsakademie Schleswig-Holstein*, sentencia del Tribunal de Justicia (Gran Sala) de 5 de junio de 2018, que se refiere a un litigio entre el *Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein* (Autoridad regional independiente de protección de datos de *Schleswig-Holstein*, Alemania; en lo sucesivo, "ULD") y *Wirtschaftsakademie Schleswig-Holstein GmbH*, sociedad de Derecho privado especializada en el ámbito de la educación que ofrece servicios de formación mediante una página de fans alojada en Facebook (en lo sucesivo *"Wirtschaftsakademie"*), respecto a la legalidad de una orden emitida por el ULD para que esta última desactivara su página de fans alojada en el sitio de la red social Facebook.

Para abordar esta contienda el TJUE tuvo en consideración los siguientes antecedentes de hecho y de derecho:

Antecedentes de hecho

Mediante resolución de fecha 3 de noviembre de 2011 (la resolución impugnada), el ULD, en su condición de autoridad de control en protección de datos, ordenó de conformidad con la *Bundesdatenschutzgesetz* (Ley Federal sobre Protección de Datos), en lo sucesivo BDSG, a *Wirtschaftsakademie,* conforme al artículo 38, apartado 5, de la BDSG, que desactivara la página de fans que había creado en Facebook en la dirección www.facebook.com/wirtschaftsakademie, bajo pena de multa coercitiva en caso de no cumplir en el plazo establecido, debido a que ni *Wirtschaftsakademie* ni Facebook informaban a los visitantes de la página de fans de que esta última recogía mediante *cookies* datos personales a su respecto y de que posteriormente trataban tales datos.

> *Artículo 38, apartado 5, de la BDSG; "Con el fin de garantizar el respeto de la presente Ley y de las demás disposiciones relativas a la protección de datos, la autoridad de control podrá ordenar la adopción de medidas dirigidas a subsanar las infracciones que se hayan constatado en la recogida, el tratamiento o la utilización de*

objetivo perseguido por una norma que regula este acceso debe guardar relación con la gravedad de la injerencia en los derechos fundamentales en cuestión que supone la operación…; (56) En efecto, conforme al principio de proporcionalidad, en el ámbito de la prevención, investigación, descubrimiento y persecución de delitos solo puede justificar una injerencia grave el objetivo de luchar contra la delincuencia que a su vez esté también calificada de "grave"; y (57) En cambio, cuando la injerencia que implica dicho acceso no es grave, puede estar justificada por el objetivo de prevenir, investigar, descubrir y perseguir "delitos en general".

> *los datos personales, o los incumplimientos técnicos u organizativos. En caso de infracciones o de incumplimientos graves, en particular cuando estos supongan un riesgo particular de vulneración del derecho a la intimidad, dicha autoridad podrá prohibir la obtención, el tratamiento o la utilización, incluso el recurso a determinados procedimientos, cuando no se hayan subsanado las infracciones o incumplimientos en un plazo razonable, incumpliéndose así la orden contemplada en la primera frase y a pesar de la aplicación de una multa coercitiva. Dicha autoridad podrá solicitar el cese del agente de protección de los datos si tal agente carece de los conocimientos o la fiabilidad necesarias para desempeñar sus funciones"*.

Las páginas de fans son cuentas de usuario que pueden ser configuradas en Facebook por particulares o empresas. Para ello, el creador de la página de fans, una vez registrado en Facebook, puede utilizar la plataforma gestionada por dicha red social para presentarse a los usuarios de esta, así como a las personas que visitan la página de fans y difundir todo tipo de comunicaciones en el mercado de los medios y de la opinión. Los administradores de páginas de fans pueden obtener estadísticas anónimas sobre los visitantes de esas páginas mediante una herramienta denominada Facebook *Insight*, que Facebook pone gratuitamente a su disposición conforme a condiciones de uso no modificables. Estos datos se recogen gracias a ficheros testigo (en lo sucesivo, «cookies»), cada uno de los cuales contiene un código de usuario único, activos durante dos años y almacenados por Facebook en el disco duro del ordenador o en cualquier otro soporte de los visitantes de la página de fans. El código de usuario, que puede vincularse a los datos de conexión de los usuarios registrados en Facebook, se recoge y trata en el momento en que se abren las páginas de fans. A este respecto, de la resolución de remisión se desprende que ni *Wirtschaftsakademie* ni Facebook Ireland Ltda. mencionaron la operación de almacenamiento y el funcionamiento de esa cookie o el tratamiento posterior de los datos, al menos durante el período del litigio.

Wirtschaftsakademie presentó una reclamación contra esta resolución alegando, en esencia, que no era responsable, a la luz del derecho aplicable a la protección de datos, ni del tratamiento de los datos realizado por Facebook, ni de las *cookies* instaladas por esta. Mediante resolución de 16 de diciembre de 2011, el ULD desestimó esta reclamación al considerar que la responsabilidad de *Wirtschaftsakademie* como proveedor de servicios estaba acreditada, argumentando que, al crear su página de fans, *Wirtschaftsakademie* había realizado una contribución activa y voluntaria a la recogida por parte de Facebook de datos personales relativos a los visitantes de dicha página de fans, datos de los que se benefició mediante estadísticas que esta última puso a su disposición.

Wirtschaftsakademie interpuso un recurso contra esta resolución ante el *Verwaltungsgericht* (Tribunal de lo Contencioso-Administrativo alemán), alegando que no le era imputable el tratamiento de datos personales efectuado por Facebook y que tampoco había encargado a Facebook, en el sentido del artículo 11 de la BDSG, que realizara un tratamiento de datos bajo su control o en el que ella pudiera influir.

El artículo 11 del BDSG, sobre recogida, tratamiento o utilización de datos personales mediante un encargado del tratamiento, presenta la siguiente redacción: "(1) Si se recogen, tratan o utilizan datos personales mediante una entidad encargada del tratamiento, quien haya encargado el tratamiento responderá de la observancia de las disposiciones de la presente Ley y demás disposiciones relativas a la protección de datos…; (2) El encargado del tratamiento deberá ser rigurosamente elegido teniendo en cuenta especialmente la adecuación de las

medidas técnicas y de organización que haya adoptado. El encargo del tratamiento requerirá forma escrita y, en particular, habrá de determinarse en detalle… Quien haya encargado el tratamiento deberá garantizar la observancia de las medidas técnicas y de organización adoptadas por el encargado del tratamiento antes del comienzo del tratamiento de los datos y, posteriormente, de forma regular. El resultado deberá quedar documentado…"

En consecuencia, *Wirtschaftsakademie* estimaba que el ULD debería haberse dirigido directamente contra Facebook en vez de adoptar en su contra la resolución impugnada. Posteriormente, según sentencia de 9 de octubre de 2013, el *Verwaltungsgericht* (Tribunal de lo Contencioso-Administrativo) anuló la resolución impugnada basándose, en esencia, en que dado que el administrador de una página de fans en Facebook no es una entidad responsable en el sentido del artículo 3, apartado 7, de la BDSG[262], *Wirtschaftsakademie* no podía ser destinataria de una medida adoptada con arreglo al artículo 38, apartado 5, de la BDSG, que dispone:

> *"Con el fin de garantizar el respeto de la presente Ley y de las demás disposiciones relativas a la protección de datos, la autoridad de control podrá ordenar la adopción de medidas dirigidas a subsanar las infracciones que se hayan constatado en la recogida, el tratamiento o la utilización de los datos personales, o los incumplimientos técnicos u organizativos. En caso de infracciones o de incumplimientos graves, en particular cuando estos supongan un riesgo particular de vulneración del derecho a la intimidad, dicha autoridad podrá prohibir la obtención, el tratamiento o la utilización, incluso el recurso a determinados procedimientos, cuando no se hayan subsanado las infracciones o incumplimientos en un plazo razonable, incumpliéndose así la orden contemplada en la primera frase y a pesar de la aplicación de una multa coercitiva. Dicha autoridad podrá solicitar el cese del agente de protección de los datos si tal agente carece de los conocimientos o la fiabilidad necesarias para desempeñar sus funciones".*

Luego, el *Oberverwaltungsgericht* (Tribunal Superior de lo Contencioso-Administrativo alemán) desestimó por infundado el recurso de apelación interpuesto por el ULD contra esa sentencia. Dicho tribunal consideró que la prohibición del tratamiento de los datos establecida en la resolución impugnada era ilegal, por cuanto el artículo 38, apartado 5, segunda frase, de la BDSG establece un procedimiento progresivo, cuya primera fase permite únicamente adoptar medidas dirigidas a subsanar las infracciones detectadas en el tratamiento de los datos. Solo se podría contemplar la prohibición inmediata del tratamiento de datos si el procedimiento para su tratamiento fuera ilícito en su totalidad y si únicamente la suspensión de ese procedimiento permitiera subsanar dicha situación. Ahora bien, según el *Oberverwaltungsgericht* (Tribunal Superior de lo Contencioso-Administrativo), no había sucedido así en el caso de autos, dado que Facebook había tenido efectivamente la posibilidad de hacer cesar las infracciones que alegó el ULD.

El *Oberverwaltungsgericht* (Tribunal Superior de lo Contencioso-Administrativo) añadió que la resolución impugnada también era ilegal debido a que solo se podía dictar una orden en virtud del artículo 38, apartado 5, de la BDSG contra la entidad responsable, en el sentido del

[262] "Se entenderá por entidad responsable toda persona o entidad que recoja, trate o utilice datos personales por cuenta propia o mediante un encargado del tratamiento".

artículo 3, apartado 7, de la BDSG, condición que no concurría en *Wirtschaftsakademie* en relación con los datos recogidos por Facebook. A su juicio, únicamente Facebook podía decidir la finalidad y los medios de la recogida y del tratamiento de los datos personales utilizados en el marco de la funcionalidad Facebook *Insights*, pues *Wirtschaftsakademie*, por su parte, solo recibía información estadística anónima.

Posteriormente, el ULD interpuso un recurso de casación ante el *Bundesverwaltungsgericht* (Tribunal Supremo de lo Contencioso-Administrativo alemán), invocando, entre otras alegaciones, una infracción del artículo 38, apartado 5, de la BDSG, así como diversos errores procesales de la resolución del tribunal de apelación. Según el ULD, la infracción cometida por *Wirtschaftsakademie* consistía en que había encargado la realización, el alojamiento y el mantenimiento de un sitio de Internet a un proveedor (concretamente, Facebook *Ireland*) que resultaba inadecuado por no haber respetado el Derecho aplicable a la protección de datos. A su entender, la orden dirigida a *Wirtschaftsakademie* mediante la resolución impugnada para que desactivara su página de fans pretendía subsanar esa infracción, pues le prohibía continuar utilizando la infraestructura de Facebook como base técnica de su sitio de Internet.

Al igual que el *Oberverwaltungsgericht* (Tribunal Superior de lo Contencioso-Administrativo), el *Bundesverwaltungsgericht* (Tribunal Supremo de lo Contencioso-Administrativo) estima que no cabe considerar que la propia *Wirtschaftsakademie* sea responsable del tratamiento de los datos, en el sentido del artículo 3, apartado 7 de la BDSG o del artículo 2, letra d), de la Directiva 95/46/CE. Este último tribunal entiende, no obstante, que dicho concepto debe, en principio, interpretarse de manera extensiva en interés de una protección efectiva del derecho a la intimidad, tal como, según afirma, ha reconocido el Tribunal de Justicia de la Unión Europea, en su jurisprudencia. Por otra parte, alberga dudas en cuanto a las facultades que tiene el ULD sobre Facebook *Germany*, habida cuenta de que el responsable de la recogida y del tratamiento de los datos personales dentro del grupo Facebook, en el ámbito de la Unión, es Facebook *Ireland.*

Por último, dicho órgano jurisdiccional se pregunta acerca de la incidencia, a efectos del ejercicio de los poderes de intervención del ULD, de las apreciaciones realizadas por la autoridad de control a la que está sujeta Facebook *Ireland* en cuanto a la legalidad del tratamiento de los datos personales en cuestión.

En estas circunstancias, el *Bundesverwaltungsgericht* (Tribunal Supremo de lo Contencioso-Administrativo) decidió suspender el procedimiento y derivar los antecedentes al TJUE, planteando una serie de cuestiones prejudiciales[263], las que pueden resumirse así:

[263] "1. ¿Debe interpretarse el artículo 2, letra d), de la Directiva [95/46] en el sentido de que regula taxativa y exhaustivamente la responsabilidad por las infracciones en materia de protección de datos, o bien, en el ámbito de las "medidas adecuadas" a que se refiere el artículo 24 de [esta Directiva] y de los "poderes efectivos de intervención" mencionados en el artículo 28, apartado 3, segundo guion, de [dicha Directiva], en las relaciones en cadena de proveedores de información también puede incurrir en responsabilidad una entidad que no sea responsable del tratamiento de los datos, en el sentido del artículo 2, letra d), de [la mencionada Directiva], por la elección del operador para ofrecer su información?; 2. ¿De la obligación impuesta por el artículo 17, apartado 2, de la Directiva [95/46] a los Estados miembros de establecer que, en caso de que se encargue el tratamiento de los datos, el responsable del tratamiento deberá "elegir un encargado del tratamiento que reúna garantías suficientes en relación con las medidas de seguridad técnica y de organización de los tratamientos que deban efectuarse" se deduce, a sensu contrario, que en otras relaciones de uso que no suponen un tratamiento de datos mediante un encargado del tratamiento en el sentido del artículo 2, letra e), de [esta Directiva] no existe tal

1. Si una entidad para promocionar su actividad, en este caso *Wirtschaftsakademie*, que utiliza una plataforma virtual o red social (encargado del tratamiento de datos), es responsable del tratamiento de los datos que dicha plataforma o red social realiza debiendo además verificar las condiciones técnicas y de seguridad que esta otorgue;

2. Hasta dónde llegan las facultades de la autoridad de control en materia de protección de datos respecto de las entidades encargadas del tratamiento que operan con filiales, en el sentido de si dicha autoridad es competente para aplicar sanciones a las mismas o solo respecto de la sociedad matriz, siempre y cuando esta se encuentre en algún Estado miembro de la Unión.

---

obligación de elección diligente y tampoco la puede imponer el Derecho nacional?; 3. En los casos en que una sociedad matriz establecida fuera de la Unión mantenga establecimientos jurídicamente independientes (filiales) en diversos Estados miembros, ¿la autoridad de control de un Estado miembro (en este caso, Alemania) es también competente con arreglo al artículo 4 y al artículo 28, apartado 6, de la Directiva [95/46] para ejercer los poderes que le otorga el artículo 28, apartado 3, de [esta Directiva] contra el establecimiento situado en su territorio, aunque dicho establecimiento solo tenga funciones de promoción y venta de espacios publicitarios así como relativas a otras medidas de marketing dirigidas a los habitantes de ese Estado miembro, mientras que, conforme al reparto de funciones dentro del grupo, corresponde al establecimiento independiente (filial) situado en otro Estado miembro (en este caso, Irlanda) la responsabilidad exclusiva relativa a la obtención y al tratamiento de los datos personales en todo el territorio de la Unión Europea y, por lo tanto, también en el otro Estado miembro (en este caso, Alemania), cuando en realidad la decisión sobre el tratamiento de los datos la toma la sociedad matriz?; 4. ¿Deben interpretarse los artículos 4, apartado 1, y 28, apartado 3, de la Directiva [95/46] en el sentido de que, en los casos en que el responsable del tratamiento disponga de un establecimiento en el territorio de un Estado miembro (en este caso, Irlanda) y de otro establecimiento jurídicamente independiente en el territorio de otro Estado miembro (en este caso, Alemania), el cual se ocupa, en particular, de la venta de espacios publicitarios, y cuya actividad está dirigida a los habitantes de dicho Estado, la autoridad de control competente en ese otro Estado miembro (en este caso, Alemania) puede adoptar medidas y dictar órdenes para la ejecución del Derecho aplicable en materia de protección de datos, incluso contra el otro establecimiento (en este caso, sito en Alemania) que, conforme al reparto interno de funciones y responsabilidades dentro del grupo, no es responsable del tratamiento de los datos, o solo puede decretar tales medidas y órdenes la autoridad de control del Estado miembro (en este caso, Irlanda) en cuyo territorio tiene su domicilio la entidad responsable dentro del grupo?; 5. ¿Deben interpretarse los artículos 4, apartado 1, letra a), y 28, apartados 3 y 6, de la Directiva [95/46] en el sentido de que, en los casos en que la autoridad de control de un Estado miembro (en este caso, Alemania) se dirige con arreglo al artículo 28, apartado 3, de [esta Directiva] contra una persona o entidad que opera en su territorio porque esta no ha elegido diligentemente al tercero implicado en el proceso de tratamiento de datos (en este caso, Facebook), dado que dicho tercero infringe el Derecho aplicable en materia de protección de datos, la autoridad de control que actúa (en este caso, Alemania) se halla vinculada a la valoración a efectos del Derecho aplicable en materia de protección de datos realizada por la autoridad de control del otro Estado miembro, donde tiene su establecimiento el tercero responsable del tratamiento de datos (en este caso, Irlanda), de manera que no puede realizar ninguna valoración jurídica diferente, o bien la autoridad de control que actúa (en este caso, Alemania) puede verificar de forma autónoma la legalidad del tratamiento de los datos realizado por el tercero establecido en el otro Estado miembro (en este caso, Irlanda) como cuestión incidental respecto de su propia actuación?; y 6. En el caso de que la autoridad de control que actúa (en este caso, Alemania) pueda efectuar una verificación de forma autónoma, ¿debe interpretarse el artículo 28, apartado 6, segunda frase, de la Directiva [95/46] en el sentido de que esta autoridad de control solo puede ejercer los poderes efectivos de intervención que le atribuye el artículo 28, apartado 3, de [esta] Directiva contra una persona o entidad establecidas en su territorio por corresponsabilidad en las infracciones en materia de protección de los datos cometidas por un tercero establecido en otro Estado miembro si, previamente, ha pedido a la autoridad de control del otro Estado miembro (en este caso, Irlanda) que ejercite sus poderes?".

Antecedentes de derecho:

Para abordar este requerimiento, el TJUE tuvo en cuenta entre otras disposiciones de la Directiva 95/46/CE, los considerandos 10, 18, 19 y 26.

> *Considerando 10 de la Directiva 95/46/CE; "Considerando que las legislaciones nacionales relativas al tratamiento de datos personales tienen por objeto garantizar el respeto de los derechos y libertades fundamentales, particularmente del derecho al respeto de la vida privada reconocido en el artículo 8 del Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales, así como en los principios generales del Derecho [de la Unión]; que, por lo tanto, la aproximación de dichas legislaciones no debe conducir a una disminución de la protección que garantizan sino que, por el contrario, debe tener por objeto asegurar un alto nivel de protección dentro de la [Unión]"*
>
> *Considerando 18 de la Directiva 95/46/CE; "Considerando que, para evitar que una persona sea excluida de la protección garantizada por la presente Directiva, es necesario que todo tratamiento de datos personales efectuado en la [Unión] respete la legislación de uno de sus Estados miembros; que, a este respecto, resulta conveniente someter el tratamiento de datos efectuados por cualquier persona que actúe bajo la autoridad del responsable del tratamiento establecido en un Estado miembro a la aplicación de la legislación de tal Estado".*
>
> *Considerando 19 de la Directiva 95/46/CE; "Considerando que el establecimiento en el territorio de un Estado miembro implica el ejercicio efectivo y real de una actividad mediante una instalación estable; que la forma jurídica de dicho establecimiento, sea una simple sucursal o una empresa filial con personalidad jurídica, no es un factor determinante al respecto; que cuando un mismo responsable esté establecido en el territorio de varios Estados miembros, en particular por medio de una empresa filial, debe garantizar, en particular para evitar que se eluda la normativa aplicable, que cada uno de los establecimientos cumpla las obligaciones impuestas por el Derecho nacional aplicable a estas actividades".*
>
> *Considerando 26 de la Directiva 95/46/CE; "Considerando que los principios de la protección deberán aplicarse a cualquier información relativa a una persona identificada o identificable; que, para determinar si una persona es identificable, hay que considerar el conjunto de los medios que puedan ser razonablemente utilizados por el responsable del tratamiento o por cualquier otra persona, para identificar a dicha persona; que los principios de la protección no se aplicarán a aquellos datos hechos anónimos de manera tal que ya no sea posible identificar al interesado; [...]".*

Así como las letras b)[264], d)[265], e)[266] y f)[267] del artículo 2 relacionado con las definiciones de determinados términos; el apartado 1 del artículo 4[268], relacionado con el derecho nacional aplicable; los apartados 1[269] y 2[270] del artículo 17 sobre la seguridad del tratamiento de datos; el artículo 24[271] relacionado con las sanciones y el artículo 28 sobre la autoridad de control.

> *Artículo 28 de la Directiva 95/46/CE; "1. Los Estados miembros dispondrán que una o más autoridades públicas se encarguen de vigilar la aplicación en su territorio de las disposiciones adoptadas por ellos en aplicación de la presente Directiva.*

---

[264] "tratamiento de datos personales" ("tratamiento"): cualquier operación o conjunto de operaciones, efectuadas o no mediante procedimientos automatizados, y aplicadas a datos personales, como la recogida, registro, organización, conservación, elaboración o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma que facilite el acceso a los mismos, cotejo o interconexión, así como su bloqueo, supresión o destrucción;

[265]"responsable del tratamiento": la persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que solo o conjuntamente con otros determine los fines y los medios del tratamiento de datos personales; en caso de que los fines y los medios del tratamiento estén determinados por disposiciones legislativas o reglamentarias nacionales o [de la Unión], el responsable del tratamiento o los criterios específicos para su nombramiento podrán ser fijados por el Derecho nacional o [de la Unión];

[266]"encargado del tratamiento": la persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que, solo o conjuntamente con otros, trate datos personales por cuenta del responsable del tratamiento;

[267] "tercero": la persona física o jurídica, autoridad pública, servicio o cualquier otro organismo distinto del interesado, del responsable del tratamiento, del encargado del tratamiento y de las personas autorizadas para tratar los datos bajo la autoridad directa del responsable del tratamiento o del encargado del tratamiento;

[268] "Los Estados miembros aplicarán las disposiciones nacionales que hayan aprobado para la aplicación de la presente Directiva a todo tratamiento de datos personales cuando: a) el tratamiento sea efectuado en el marco de las actividades de un establecimiento del responsable del tratamiento en el territorio del Estado miembro. Cuando el mismo responsable del tratamiento esté establecido en el territorio de varios Estados miembros deberá adoptar las medidas necesarias para garantizar que cada uno de dichos establecimientos cumple las obligaciones previstas por el Derecho nacional aplicable; b)el responsable del tratamiento no esté establecido en el territorio del Estado miembro, sino en un lugar en que se aplica su legislación nacional en virtud del Derecho internacional público; c) el responsable del tratamiento no esté establecido en el territorio de la [Unión] y recurra, para el tratamiento de datos personales, a medios, automatizados o no, situados en el territorio de dicho Estado miembro, salvo en caso de que dichos medios se utilicen solamente con fines de tránsito por el territorio de la [Unión]".

[269] "Los Estados miembros establecerán la obligación del responsable del tratamiento de aplicar las medidas técnicas y de organización adecuadas, para la protección de los datos personales contra la destrucción, accidental o ilícita, la pérdida accidental y contra la alteración, la difusión o el acceso no autorizados, en particular cuando el tratamiento incluya la transmisión de datos dentro de una red, y contra cualquier otro tratamiento ilícito de datos personales.

Dichas medidas deberán garantizar, habida cuenta de los conocimientos técnicos existentes y del coste de su aplicación, un nivel de seguridad apropiado en relación con los riesgos que presente el tratamiento y con la naturaleza de los datos que deban protegerse".

[270] "Los Estados miembros establecerán que el responsable del tratamiento, en caso de tratamiento por cuenta del mismo, deberá elegir un encargado del tratamiento que reúna garantías suficientes en relación con las medidas de seguridad técnica y de organización de los tratamientos que deban efectuarse, y se asegure de que se cumplen dichas medidas".

[271] "Los Estados miembros adoptarán las medidas adecuadas para garantizar la plena aplicación de las disposiciones de la presente Directiva y determinarán, en particular, las sanciones que deben aplicarse en caso de incumplimiento de las disposiciones adoptadas en ejecución de la presente Directiva".

> *Estas autoridades ejercerán las funciones que les son atribuidas con total independencia.*
> *2. Los Estados miembros dispondrán que se consulte a las autoridades de control en el momento de la elaboración de las medidas reglamentarias o administrativas relativas a la protección de los derechos y libertades de las personas en lo que se refiere al tratamiento de datos de carácter personal.*
> *3. La autoridad de control dispondrá, en particular, de: poderes de investigación, como el derecho de acceder a los datos que sean objeto de un tratamiento y el de recabar toda la información necesaria para el cumplimiento de su misión de control; poderes efectivos de intervención, como, por ejemplo, el de formular dictámenes antes de realizar los tratamientos, con arreglo al artículo 20, y garantizar una publicación adecuada de dichos dictámenes, o el de ordenar el bloqueo, la supresión o la destrucción de datos, o incluso prohibir provisional o definitivamente un tratamiento, o el de dirigir una advertencia o amonestación al responsable del tratamiento o el de someter la cuestión a los parlamentos u otras instituciones políticas nacionales; capacidad procesal en caso de infracciones a las disposiciones nacionales adoptadas en aplicación de la presente Directiva o de poner dichas infracciones en conocimiento de la autoridad judicial. Las decisiones de la autoridad de control lesivas de derechos podrán ser objeto de recurso jurisdiccional…Toda autoridad de control será competente, sean cuales sean las disposiciones de Derecho nacional aplicables al tratamiento de que se trate, para ejercer en el territorio de su propio Estado miembro los poderes que se le atribuyen en virtud del apartado 3 del presente artículo. Dicha autoridad podrá ser instada a ejercer sus poderes por una autoridad de otro Estado miembro… Las autoridades de control cooperarán entre sí en la medida necesaria para el cumplimiento de sus funciones, en particular mediante el intercambio de información que estimen útil".*

En los considerandos de la sentencia el TJUE determina que la creación de una página de fans en Facebook implica por parte de su administrador una acción de configuración, en función, entre otros aspectos, de su audiencia destinataria, así como de los objetivos de gestión o de promoción de sus actividades, que influye en el tratamiento de datos personales a efectos de la elaboración de las estadísticas establecidas a partir de las visitas que dicha página tenga. Así el administrador puede, gracias a los filtros que Facebook pone a su disposición, definir criterios para elaborar esas estadísticas e incluso designar las categorías de personas cuyos datos personales serán objeto de explotación por parte de Facebook. Por consiguiente, el administrador de una página de fans alojada en Facebook contribuye al tratamiento de los datos personales de los visitantes de su página.

El administrador de la página de fans puede solicitar la obtención y, por tanto, el tratamiento, de datos demográficos relativos a su audiencia destinataria, especialmente, de las tendencias en materia de edad, sexo, situación sentimental y profesión, información sobre el estilo de vida y los intereses de su audiencia destinataria, así como información relativa a las compras y comportamiento de compras en línea de los visitantes de su página, las categorías de productos o servicios que más les interesan, además de datos geográficos que permiten al administrador de la página de fans saber dónde efectuar promociones especiales u organizar eventos y, con carácter más general, dirigir de forma óptima su oferta de información.

Si bien las estadísticas de audiencia elaboradas por Facebook se transmiten únicamente al administrador de la página de fans de forma anónima, la elaboración de esas estadísticas se basa en la recogida previa, mediante *cookies* instaladas por Facebook en los ordenadores o cualquier otro aparato de las personas que visitan esas páginas, y en el tratamiento de los datos personales de esos visitantes a los citados efectos estadísticos. En cualquier caso, la Directiva 95/46/CE no exige, cuando existe una responsabilidad conjunta de varios operadores respecto a un mismo tratamiento, que cada uno de ellos tenga acceso a los datos personales en cuestión.

En estas circunstancias, señala el Tribunal, procede considerar que el administrador de una página de fans alojada en Facebook, como *Wirtschaftsakademie*, participa, mediante su acción de configuración, en función, en particular, de su audiencia destinataria, así como de objetivos de gestión o de promoción de sus actividades, en la determinación de los fines y los medios del tratamiento de los datos personales de los visitantes de su página de fans.

Por lo que el TJUE establece que, dicho administrador debe ser calificado en el presente caso como responsable de ese tratamiento en la Unión, en el sentido del artículo 2, letra d), de la Directiva 95/46/CE, conjuntamente con Facebook *Ireland* y por consiguiente no se encuentra eximido de sus obligaciones en materia de protección de datos personales, siendo en definitiva conjuntamente responsables del tratamiento de datos tanto el operador de la red social como el administrador de una página de fans alojada en esa red.

Incluso las páginas de fans alojadas en Facebook pueden ser visitadas igualmente por personas que no son usuarias de Facebook y que, por tanto, no disponen de una cuenta de usuario en esa red social. En ese caso, la responsabilidad del administrador de la página de fans respecto del tratamiento de los datos personales de tales personas resulta aún mayor, pues la mera consulta de la página de fans por parte de los visitantes desencadena automáticamente el tratamiento de sus datos personales.

Sobre la competencia de la autoridad de control, en este caso ULD, es preciso recordar que según el artículo 28, apartados 1 y 3, de la Directiva 95/46/CE, cada autoridad de control ejerce todas las facultades que se le han conferido, de conformidad al derecho nacional, en el territorio de su propio Estado miembro, a fin de garantizar en dicho territorio el respeto de las normas en materia de protección de datos[272]. Cuestión que hay que entender armónicamente con la letra a) del apartado 1 del artículo 4 de dicha Directiva, en el sentido de que cuando el mismo responsable del tratamiento esté establecido en el territorio de varios Estados miembros, deberá adoptar las medidas necesarias para garantizar que cada uno de dichos establecimientos cumpla las obligaciones previstas por el derecho nacional aplicable.

En el caso en análisis, consta que Facebook Inc., es responsable del tratamiento de datos personales, conjuntamente con Facebook *Ireland*, que dispone de un establecimiento estable en Alemania, a saber, Facebook *Germany*, situado en Hamburgo, y que esta última sociedad ejerce real y efectivamente actividades en dicho Estado miembro. Por lo tanto, constituye un establecimiento en el sentido del artículo 4, apartado 1, letra a), de la Directiva 95/46/CE, siendo también la autoridad de control alemana competente, conforme al artículo 28, apartado 1, de la referida Directiva, para aplicar este Derecho a dicho tratamiento.

El TJUE precisa que cuando una empresa establecida fuera de la Unión dispone de varios establecimientos en diversos Estados miembros, la autoridad de control de un Estado miembro

[272] Ver la sentencia de 1 de octubre de 2015, *Weltimmo*, C-230/14, EU: C: 2015:639, apartado 51.

está facultada para ejercer los poderes que le confiere el artículo 28, apartado 3, de la mencionada Directiva respecto a un establecimiento de esa empresa situado en el territorio de ese Estado miembro, aun cuando, en virtud del reparto de funciones dentro del grupo, por un lado, este establecimiento únicamente se encarga de la venta de espacios publicitarios y de otras actividades de marketing en el territorio de dicho Estado miembro y, por otro lado, la responsabilidad exclusiva de la recogida y del tratamiento de los datos personales incumbe, para todo el territorio de la Unión, a un establecimiento situado en otro Estado miembro.

El Tribunal reafirma así que toda autoridad nacional de control está habilitada y por consiguiente es competente para comprobar si un tratamiento de datos personales en el territorio del Estado miembro de esa autoridad respeta las exigencias establecidas por la Directiva 95/46/CE[273]. Por lo que el ULD está facultado para apreciar, de manera autónoma respecto de las evaluaciones efectuadas por la autoridad de control irlandesa, la legalidad del tratamiento de datos controvertido.

Sentencia C-25/17 Jehovan Todistajat, de 10 de julio de 2018

La cuarta sentencia, individualizada C-25/17 *Jehovan todistajat*, sentencia del Tribunal de Justicia (Gran Sala) de 10 de julio de 2018, se relaciona con la actividad religiosa que realizan los Testigos de Jehová en Finlandia.

Los hechos pueden resumirse de la siguiente manera: el 17 de septiembre de 2013, la Comisión de Protección de Datos de Finlandia[274], de conformidad a los dispuesto en su Ley de Protección de Datos N° 523/1999[275], adoptó, a instancias del Supervisor de Protección de Datos[276], una resolución mediante la cual prohibía a la comunidad de los Testigos de Jehová recoger o tratar datos personales en relación con la actividad de predicación puerta a puerta llevada a cabo por sus miembros sin que concurrieran los requisitos legales para el tratamiento de tales datos. Además, la Comisión de Protección de Datos impuso a dicha comunidad, de conformidad con el artículo 44, apartado 2, de la misma Ley, la obligación de dejar de recoger, dentro de un plazo de seis meses, datos personales para los fines de la comunidad sin cumplir los citados requisitos[277].

La comunidad de los Testigos de Jehová recurrió dicha resolución ante el *Helsingin hallinto-oikeus* (Tribunal de lo Contencioso Administrativo de *Helsinki* de Finlandia), el cual, mediante sentencia de 18 de diciembre de 2014, anuló la resolución recurrida, señalando que la comunidad de los Testigos de Jehová no es responsable del tratamiento de datos personales, en el sentido de la Ley 523/1999, y que la actividad de dicha comunidad no constituye un

[273] Ver sentencia de 6 de octubre de 2015, *Schrems,* C-362/14, EU:C:2015:650, apartado 47.

[274] tietosuojalautakunta.

[275] La Directiva 95/46/CE fue incorporada al Derecho finlandés mediante la *Henkilötietolaki* 523/1999, que es la Ley de Datos Personales (523/1999); en lo sucesivo Ley 523/1999.

[276] tietosuojavaltuutettu.

[277] Según el señalado artículo 44, apartado 2, la Comisión de Protección de Datos, a solicitud del Supervisor de Protección de Datos, podrá prohibir el tratamiento de datos personales que vulnere dicha Ley o los reglamentos u otras disposiciones adoptadas en virtud de dicha Ley, así como ordenar la subsanación dentro de un plazo razonable en caso de acción u omisión ilegales.

tratamiento ilícito de tales datos. El Supervisor de protección de datos recurrió dicha sentencia ante el *Korkein hallinto-oikeus* (Tribunal Supremo de lo Contencioso Administrativo de Finlandia), el que decidió suspender el procedimiento remitiendo los antecedentes al TJUE, planteando diversas cuestiones prejudiciales;

> *"1. ¿Deben interpretarse las excepciones al ámbito de aplicación de la Directiva [95/46] establecidas en el artículo 3, apartado 2, guiones primero y segundo, de esta en el sentido de que la recogida y demás operaciones de tratamiento de datos personales efectuadas por miembros de una comunidad religiosa en relación con la actividad de predicación puerta a puerta no están comprendidas en el ámbito de aplicación de la Directiva? A efectos de evaluar la aplicabilidad de la Directiva [95/46], ¿qué relevancia tiene, por un lado, que la actividad de predicación en cuyo marco se recogen los datos sea organizada por la comunidad religiosa y sus congregaciones y, por otro, que se trate al mismo tiempo de la práctica religiosa personal de los miembros de la comunidad religiosa?*
> *2. ¿Debe interpretarse la definición del concepto de "fichero" establecida en el artículo 2, letra c), de la Directiva [95/46], habida cuenta de los considerandos 26 y 27 de dicha Directiva, en el sentido de que el conjunto de los datos personales recopilados de forma no automatizada en relación con la actividad descrita de predicación puerta a puerta (nombre, dirección y otros posibles datos y características relativos a la persona): a) no constituye un fichero en tal sentido porque no se trata de archivos de fichas o catálogos específicos ni de sistemas similares de clasificación y búsqueda a efectos de la definición de la Ley [523/1999], o bien y b) constituye un fichero en tal sentido porque de dichos datos, teniendo en cuenta su finalidad, puede extraerse la información necesaria para un uso posterior de forma efectivamente sencilla y sin un coste excesivo, tal y como está previsto en la Ley [523/1999]?*
> *3. ¿Debe interpretarse la expresión "que solo o conjuntamente con otros determine los fines y medios del tratamiento de datos personales", mencionada en el artículo 2, letra d), de la Directiva [95/46], en el sentido de que una comunidad religiosa que organiza una actividad en la que se recogen datos personales (en particular, mediante el reparto de las zonas asignadas a los predicadores, mediante el seguimiento de la actividad de predicación y mediante la llevanza de registros sobre las personas que no desean que los predicadores vayan a sus domicilios) puede ser considerada responsable del tratamiento de datos personales en relación con esta actividad de sus miembros, pese a que la comunidad religiosa alega que solo determinados predicadores tienen acceso a la información registrada?*
> *4. ¿Debe interpretarse el artículo 2, letra d), de la Directiva [95/46] en el sentido de que la comunidad religiosa solo puede ser considerada responsable del tratamiento si adopta otras medidas específicas, como encargos o instrucciones por escrito, mediante las que dirige la recogida de datos, o bien basta con que la comunidad religiosa desempeñe un papel efectivo en la dirección de la actividad de sus miembros?".*

Estas cuestiones prejudiciales son posibles de sintetizar de la siguiente manera:

1. Si proceden o no las excepciones sobre el ámbito de aplicación de la Directiva 95/46/CE, establecidas en la misma, en el apartado 2 del artículo 3, en el sentido de si sus disposiciones no le son aplicables a una congregación religiosa o si estas

actividades se enmarcan en aquellas que son personales o domesticas de las personas físicas.

2. En segundo lugar, el tribunal remitente, plantea ante el TJUE cuál es la significancia y alcance del concepto de fichero, al que alude la letra c) del artículo 2 de la Directiva 95/46/CE, en el sentido de si la actividad puerta a puerta que realizan distintos integrantes de dicha congragación religiosa, en la que obtienen de forma no automatizada, diversos datos, tales como nombre, dirección u otros, puede o no incluirse en la expresión fichero de datos.

3. Y, en tercer lugar, si una comunidad religiosa, en este caso los Testigos de Jehová, en su labor de puerta a puerta y de predicación en general, al recoger información o datos personales de con quienes interactúan en tales labores, puede ser considerada como responsable del tratamiento, al que alude la letra d) del artículo 2 de la Directiva 95/46/CE.

Un aspecto para considerar es que todas las cuestiones plantadas, se relacionan, según el tribunal remitente, con el apartado 1 del artículo 10 de la Carta de Derechos Fundamentales de la Unión Europea CDFUE, que establece: *"Toda persona tiene derecho a la libertad de pensamiento, de conciencia y de religión. Este derecho implica la libertad de cambiar de religión o de convicciones, así como la libertad de manifestar su religión o sus convicciones individual o colectivamente, en público o en privado, a través del culto, la enseñanza, las prácticas y la observancia de los ritos"*.

El derecho garantizado en el apartado 1 corresponde al derecho garantizado en el artículo 9 del CEDH y, de conformidad con lo dispuesto en el apartado 3 del artículo 52 de la Carta, tiene el mismo sentido y alcance. Por lo tanto, las limitaciones deben respetar el apartado 2 de dicho artículo 9, redactado como sigue: "La libertad de manifestar su religión o sus convicciones no puede ser objeto de más restricciones que las que, previstas por la ley, constituyen medidas necesarias, en una sociedad democrática, para la seguridad pública, la protección del orden, de la salud o de la moral públicas, o la protección de los derechos o las libertades de los demás."

Para la resolución de esta controversia el TJUE, tiene en consideración diversas disposiciones de la Directiva 95/46/CE, varias de las cuales ya se han explicado y transcrito a lo largo de este trabajo, por lo que nos referiremos solo a algunas de ellas. En efecto, sobre el marco jurídico aplicable el Tribunal revisa los considerandos 10, 12[278], 15[279], 26 y 27[280] de la señalada

[278] "Considerando que los principios de la protección deben aplicarse a todos los tratamientos de datos personales cuando las actividades del responsable del tratamiento entren en el ámbito de aplicación del Derecho comunitario; que debe excluirse el tratamiento de datos efectuado por una persona física en el ejercicio de actividades exclusivamente personales o domésticas, como la correspondencia y la llevanza de un repertorio de direcciones"

[279] "Considerando que los tratamientos que afectan a dichos datos solo quedan amparados por la presente Directiva cuando están automatizados o cuando los datos a que se refieren se encuentran contenidos o se destinan a encontrarse contenidos en un archivo estructurado según criterios específicos relativos a las personas, a fin de que se pueda acceder fácilmente a los datos de carácter personal de que se trata";

[280] "Considerando que la protección de las personas debe aplicarse tanto al tratamiento automático de datos como a su tratamiento manual; que el alcance de esta protección no debe depender, en efecto, de las técnicas utilizadas,

Directiva, además de los artículos 1 (apartado 1), 2 letras a), b), c) y d) y 3 (apartado 2)[281]. De igual forma se analizan las disposiciones contenidas en la Ley de protección de datos de Finlandia 523/1999.

Sobre la primera cuestión planteada

En relación a la aplicación o no de la Directiva 95/46/CE a una congregación religiosa o de sus miembros, como los Testigos de Jehová y si estas actividades se enmarcan o no dentro de actividades personales o domésticas que eximen a las personas físicas de la aplicación de sus disposiciones, el TJUE señala que la recogida de datos personales por miembros de dicha comunidad constituye una actividad de particulares, por consiguiente, no se trata de una actividad propia de las autoridades estatales y, por tanto, no puede asimilarse a las actividades mencionadas en el artículo 3, apartado 2, primer guion, de la Directiva 95/46/CE.

En lo referente a las actividades personales o domésticas a que se refiere el segundo guion del apartado 2 del artículo 3 de la señalada Directiva, el Tribunal señala que la exigencia normativa es que trate del ejercicio de actividades "exclusivamente" personales o domésticas[282] y agrega que la expresión "personales o domésticas", se refiere a la actividad de la persona que trata los datos personales, no a la persona cuyos datos son tratados[283].

Además, la actividad de predicación puerta a puerta, donde los miembros de la comunidad de los Testigos de Jehová recogen datos personales, tiene por objeto, por su propia naturaleza, difundir la fe de dicha comunidad a personas que no pertenecen al hogar de los miembros predicadores. Por lo tanto, dicha actividad está dirigida hacia el exterior de la esfera privada de los integrantes que predican. De igual forma, los predicadores transmiten algunos de los datos que recogen, a las congregaciones de su comunidad, las que, con dichos datos, llevan registros de las personas que visitan, permitiendo a un número potencialmente indeterminado de personas el acceso a algunos de los datos recogidos.

---

pues lo contrario daría lugar a riesgos graves de elusión; que, no obstante, por lo que respecta al tratamiento manual, la presente Directiva solo abarca los ficheros, y no se aplica a las carpetas que no están estructuradas; que, en particular, el contenido de un fichero debe estructurarse conforme a criterios específicos relativos a las personas, que permitan acceder fácilmente a los datos personales; que, de conformidad con la definición que recoge la letra c) del artículo 2, los distintos criterios que permiten determinar los elementos de un conjunto estructurado de datos de carácter personal y los distintos criterios que regulan el acceso a dicho conjunto de datos pueden ser definidos por cada Estado miembro; que las carpetas y conjuntos de carpetas, así como sus portadas, que no estén estructuradas conforme a criterios específicos no están comprendidas en ningún caso en el ámbito de aplicación de la presente Directiva".

[281]"Las disposiciones de la presente Directiva no se aplicarán al tratamiento de datos personales:

efectuado en el ejercicio de actividades no comprendidas en el ámbito de aplicación del Derecho comunitario, como las previstas por las disposiciones de los títulos V y VI del Tratado de la Unión Europea y, en cualquier caso, al tratamiento de datos que tenga por objeto la seguridad pública, la defensa, la seguridad del Estado (incluido el bienestar económico del Estado cuando dicho tratamiento esté relacionado con la seguridad del Estado) y las actividades del Estado en materia penal;

efectuado por una persona física en el ejercicio de actividades exclusivamente personales o domésticas".

[282] Ver la sentencia de 11 de diciembre de 2014, Ryneš, C-212/13, EU: C: 2014:2428, apartado 30.

[283] Ver en este sentido, la sentencia de 11 de diciembre de 2014, Ryneš, C-212/13, EU: C: 2014:2428, apartados 31 y 33.

En cuanto al hecho de que el tratamiento de datos personales se lleve a cabo en el ámbito de una actividad vinculada a una práctica religiosa configurando una acción de carácter exclusivamente personal es importante recordar, que aun cuando el artículo 10 apartado 1 de la CDFUE protege en un sentido amplio la libertad religiosa, esta protección o tutela no le confiere a dicha actividad, el carácter exclusivamente personal o doméstico a efectos del artículo 3, apartado 2, segundo guion, de la Directiva 95/46.

Por lo demás, la libertad de manifestar su religión individual o colectivamente, en público o en privado, puede adoptar diversas formas, como la enseñanza, las prácticas y la observancia de los ritos, dicha libertad conlleva igualmente el derecho de intentar convencer a otras personas, por ejemplo, mediante la predicación[284].

Hay que recordar que el derecho a la libertad de conciencia y de religión, consagrado en el artículo 10, apartado 1 de la Carta, implica, en particular, la libertad de toda persona de manifestar su religión o sus convicciones individual o colectivamente, en público o en privado, a través del culto, la enseñanza, las prácticas y la observancia de los ritos. La Carta recoge una acepción amplia del concepto de religión, comprensiva tanto del *forum internum*, es decir, del hecho de tener convicciones, como del *forum externum*, es decir, de la manifestación pública de la fe religiosa[285].

En definitiva, el Tribunal concluye que ninguna de las acciones realizadas tanto por el o los predicadores, como por la congregación religiosa Testigos de Jehová, configuran algunos de los supuestos previstos en el apartado 2 del artículo 3 de la Directiva 95/46/CE y por consiguiente sus disposiciones le son plenamente aplicables.

Sobre la segunda cuestión planteada

En relación a la controversia puesta en conocimiento del TJUE por el remitente, relativa al sentido y alcance del término "fichero", es importante volver a precisar que en el artículo 2 de la Directiva 95/46/CE se establecen una serie de definiciones, y precisamente su letra c) señala que el concepto fichero o fichero de datos personales es "todo conjunto estructurado de datos personales, accesibles con arreglo a criterios determinados, ya sea centralizado, descentralizado o repartido de forma funcional o geográfica", es decir, la Directiva entrega una definición amplia de fichero, incluyendo tanto el tratamiento manual[286] como automatizado de los datos tratados.

Esta amplitud de la noción de fichero se desprende de los considerandos 15 y 27 de la Directiva 95/46/CE.

> *Considerando 15: "Considerando que los tratamientos que afectan a dichos datos sólo quedan amparados por la presente Directiva cuando están automatizados o cuando*

[284] Ver sentencias de 25 de mayo de 1993, Kokkinakis c. Grecia, CE: ECHR:1993:0525JUD001430788, § 31, y de 8 de noviembre de 2007, Perry c. Letonia, CE: ECHR:2007:1108JUD003027303, § 52, del TEDH.

[285] Ver sentencia de 29 de mayo de 2018, Liga van Moskeeën en Islamitische Organisaties Provincie Antwerpen y otros, C-426/16, EU:C:2018:335, apartado 44.

[286] En el caso de los tratamientos manuales de datos personales, solo cuando los datos tratados estén incluidos o destinados a ser incluidos en un fichero.

> *los datos a que se refieren se encuentran contenidos o se destinan a encontrarse contenidos en un archivo estructurado según criterios específicos relativos a las personas, a fin de que se pueda acceder fácilmente a los datos de carácter personal de que se trata".*
>
> *Considerando 27:"Considerando que la protección de las personas debe aplicarse tanto al tratamiento automático de datos como a su tratamiento manual; que el alcance de esta protección no debe depender, en efecto, de las técnicas utilizadas, pues la contrario daría lugar a riesgos graves de alusión; que, no obstante, por lo que respecta al tratamiento manual, la presente Directiva sólo abarca los ficheros, y no se aplica a las carpetas que no están estructuradas; que, en particular, el contenido de un fichero debe estructurarse conforme a criterios específicos relativos a las personas, que permitan acceder fácilmente a los datos personales; que, de conformidad con la definición que recoge la letra c) del artículo 2, los distintos criterios que permiten determinar los elementos de un conjunto estructurado de datos de carácter personal y los distintos criterios que regulan el acceso a dicho conjunto de datos pueden ser definidos por cada Estado miembro; que, las carpetas y conjuntos de carpetas, así como sus portadas, que no estén estructuradas conforme a criterios específicos no están comprendidas en ningún caso en el ámbito de aplicación de la presente Directiva".*

Esta amplitud se refuerza en que la Directiva, tampoco se refiere a las modalidades de estructuración del fichero ni la forma que este debe revestir. En particular, no se deduce del citado precepto ni de ninguna otra disposición de dicha Directiva que, para poder apreciar la existencia de un fichero, los datos personales en cuestión deban figurar en fichas, en catálogos específicos o en otro sistema de búsqueda.

Como en el caso en análisis, los tratamientos de datos personales se efectúan de manera no automatizada, se plantea la interrogante de si los datos tratados están incluidos o destinados a ser incluidos en un fichero, a efectos del artículo 2, letra c), y del artículo 3, apartado 1, de la Directiva 95/46/CE.

En el caso en análisis, se desprende que la recogida de datos en relación con la actividad de predicación puerta a puerta se realiza a modo de recordatorio, sobre la base de un reparto por zonas geográficas, con el fin de facilitar la organización de visitas posteriores a personas que ya han sido contactadas. Dichos datos no solo comprenden información sobre el contenido de las conversaciones acerca de las convicciones de la persona contactada, sino también su nombre y dirección. Además, esa información, o al menos parte de esta, se utiliza para elaborar registros, gestionados por las congregaciones de la comunidad de los Testigos de Jehová, sobre las personas que no desean recibir más visitas de miembros predicadores de dicha comunidad. Así entonces, el nombre y la dirección de las personas contactadas, sus convicciones o su deseo de no recibir más visitas, se seleccionan de forma que permitan recuperar fácilmente los datos relativos a determinadas personas.

Por consiguiente, el TJUE concluye que el artículo 2, letra c), de la Directiva 95/46/CE debe interpretarse en el sentido de que el concepto de fichero, definido en esa disposición, comprende un conjunto de datos personales recogidos en relación con una actividad de predicación puerta a puerta, consistentes en nombres, direcciones y otra información relativa a las personas contactadas, siempre que los datos estén estructurados según criterios

determinados que permitan, en la práctica, recuperarlos fácilmente para su utilización posterior. Para que dicho conjunto de datos esté comprendido en ese concepto no es preciso que incluya fichas, catálogos específicos u otros sistemas de búsqueda.

Sobre la tercera cuestión planteada

Sobre si se considera que una comunidad religiosa es responsable, junto con sus miembros predicadores, de los tratamientos de datos personales efectuados en relación con una actividad de predicación organizada por dicha comunidad en los términos que prevé expresamente el artículo 2, letra d), de la Directiva 95/46/CE, en el sentido de que el responsable del tratamiento considera a la persona física o jurídica que, sola o conjuntamente con otros, determine los fines y los medios del tratamiento de datos personales.

En consecuencia, dicho concepto no se refiere necesariamente a una única persona física o jurídica, sino que puede concernir a varios agentes que participen en ese tratamiento, cada uno de los cuales estará por tanto sujeto a las disposiciones aplicables en materia de protección de datos[287], estableciendo una concepción amplia del responsable, en que dichos agentes estén afectos a distintos grados de responsabilidad, dependiendo de la etapa del tratamiento en la que estén involucrados.

De igual forma ni la señalada letra d) del artículo 2 de la Directiva, ni ninguna otra de sus disposiciones considera que la determinación de los fines y de los medios del tratamiento deba efectuarse mediante instrucciones por escrito o consignas impartidas por el responsable del tratamiento. En cambio, una persona física o jurídica que influye en el tratamiento de datos personales y participa, por tanto, en la determinación de los fines y los medios del tratamiento puede ser considerada responsable del tratamiento en el sentido del artículo 2, letra d), de la Directiva 95/46/CE.

En consecuencia, el TJUE, considera que una comunidad religiosa es responsable, junto con sus miembros predicadores, de los tratamientos de datos personales efectuados por estos últimos en relación con una actividad de predicación puerta a puerta organizada, coordinada y fomentada por dicha comunidad, en este caso los Testigos de Jehová, sin que sea necesario que la comunidad tenga acceso a los datos ni haga falta demostrar que la comunidad ha impartido a sus miembros instrucciones por escrito o consignas respecto a esos tratamientos.

Sentencia C-40/17- Fashion ID, de 29 de julio de 2019

Siguiendo con el orden cronológico, el quinto fallo a analizar es el individualizado C-40/17- *Fashion ID*, sentencia del Tribunal de Justicia (sala segunda) de 29 de julio de 2019. *Fashion ID GmbH & Co. KG* contra *Verbraucherzentrale NRW EV*, cuyos hechos pueden resumirse de la siguiente manera:

Fashion ID, empresa de comercio electrónico que se dedica a la venta de prendas de vestir, insertó en su sitio de Internet el módulo social "me gusta" de la red social Facebook (en lo sucesivo, botón "me gusta" de Facebook). Así, cuando un visitante consulta el sitio de Internet

[287] Ver en este sentido, la sentencia de 5 de junio de 2018, *Wirtschaftsakademie Schleswig-Holstein*, C-210/16, EU:C:2018:388, apartado 29.

de *Fashion ID*, se transmiten a Facebook *Ireland* datos personales de ese visitante, debido a que dicho sitio incorpora el citado botón. Esa transmisión se efectúa sin que el visitante del sitio sea consciente de ello y con independencia de si es miembro de la red social Facebook o de si clicó en el botón "me gusta" de Facebook.

Una característica propia de Internet consiste en permitir que el navegador del visitante de un sitio de Internet presente contenidos de distintas fuentes. Así, por ejemplo, fotos, videos, actualidades y el botón "me gusta" de Facebook de que se trata en el presente caso pueden estar vinculados a un sitio de Internet y figurar en él. Si el administrador de un sitio de Internet pretende insertar esos contenidos externos, coloca en dicho sitio un vínculo que remite al contenido externo. Cuando el navegador del visitante de dicho sitio abre ese vínculo, solicita el contenido externo y lo inserta en el lugar deseado de exposición del sitio. A tal fin, el navegador transmite al servidor del proveedor externo, la dirección IP del ordenador de dicho visitante y los datos técnicos del navegador para que el servidor pueda determinar en qué formato se suministra el contenido a esa dirección. El navegador transmite además información sobre el contenido deseado. El administrador de un sitio de Internet que ofrece un contenido externo insertándolo en dicho sitio no tiene capacidad para determinar los datos que el navegador transmite ni lo que el proveedor externo hace de esos datos, en particular, si decide almacenarlos y analizarlos.

Verbraucherzentrale NRW, asociación de utilidad pública de defensa de los intereses de los consumidores, reprocha a *Fashion ID* haber transmitido a Facebook *Ireland* datos de carácter personal pertenecientes a los visitantes de su sitio de Internet, por un lado, sin el consentimiento de estos últimos y, por otro, incumpliendo las obligaciones de información establecidas en las disposiciones relativas a la protección de los datos personales, por lo que ejercitó una acción de cesación ante el *Landgericht Düsseldorf* (Tribunal Regional de lo Civil y Penal de *Düsseldorf*, Alemania) en contra de *Fashion ID* con el objeto de que esta última pusiera fin a dicha práctica.

Mediante resolución de 9 de marzo de 2016, el *Landgericht Düsseldorf* (Tribunal Regional de lo Civil y Penal de *Düsseldorf*) estimó parcialmente las pretensiones de *Verbraucherzentrale NRW*, tras reconocer su legitimación activa según se dispone en la *Gesetz gegen den unlauteren Wettbewerb* (Ley contra la Competencia Desleal), en lo sucesivo UWG, que así lo establece en su artículo 8, apartado 3, punto 3 al señalar: "Las acciones a las que hace referencia el apartado 1[288] podrán ser ejercitadas: "... 3. Por las entidades habilitadas que demuestren estar incluidas en la lista de entidades habilitadas de conformidad con el artículo 4 de la *Unterlassungsklagengesetz* (Ley sobre las Acciones de Cesación) o en la lista de la Comisión Europea mencionada en el artículo 4, apartado 3, de la Directiva 2009/22[289]".

Fashion ID apeló dicha resolución ante el *Oberlandesgericht Düsseldorf* (Tribunal Superior Regional de lo Civil y Penal de *Düsseldorf*, Alemania), argumentando que la resolución del

[288] "1) Podrá ejercitarse una acción de cesación y, en caso de riesgo de reiteración, una acción de prohibición contra quien realice una práctica comercial ilícita con arreglo a los artículos 3 o 7. La acción de prohibición podrá ejercitarse desde el momento en que exista un riesgo de que se produzca tal infracción de los artículos 3 o 7…"

[289] Directiva 2009/22/CE del Parlamento Europeo y del Consejo, de 23 de abril de 2009, relativa a las acciones de cesación en materia de protección de los intereses de los consumidores (DO 2009, L 110, p. 30), en su versión modificada por el Reglamento (UE) n.º 524/2013 del Parlamento Europeo y del Consejo, de 21 de mayo de 2013 (DO 2013, L 165, p. 1) (en lo sucesivo, Directiva 2009/22).

Tribunal Regional de lo Civil y Penal de primera instancia no es compatible con la Directiva 95/46/CE. Por un lado, *Fashion ID* alega que los artículos 22[290] a 24[291] de dicha Directiva únicamente contemplan vías de recurso en favor de los afectados por el tratamiento de los datos personales y de las autoridades de control competentes. En consecuencia, considera que la acción judicial ejercitada por *Verbraucherzentrale NRW* no es admisible debido a que esta asociación no está legitimada para ejercitar acciones judiciales en el marco de la Directiva 95/46/CE[292].

Por otro lado, *Fashion ID* considera que el *Landgericht Düsseldorf* (Tribunal Regional de lo Civil y Penal de Düsseldorf) la declaró erróneamente responsable del tratamiento, en el sentido del artículo 2, letra d), de la Directiva 95/46/CE, en la medida en que no tiene influencia alguna en los datos transmitidos por el navegador del visitante de su sitio de Internet ni en el hecho de si Facebook *Ireland* los va a utilizar y cómo va a hacerlo en su caso.

En estas circunstancias, el *Oberlandesgericht Düsseldorf* (Tribunal Superior Regional de lo Civil y Penal de Düsseldorf) decidió suspender el procedimiento y plantear al TJUE una serie de cuestiones prejudiciales, las que se resumen en las siguientes:

1. Si se reconoce o no a las asociaciones de utilidad pública para la protección de los intereses de los consumidores, la facultad de actuar contra el infractor de la normativa sobre protección de datos personales, principalmente según lo disponen los artículos 22, 23 y 24 de la Directiva 95/46/CE.

2. Determinar si una empresa como *Fashion ID* en las circunstancias propias de la controversia, puede ser considerada como responsable del tratamiento, en el sentido del artículo 2, letra d), de la Directiva 95/46/CE, aunque esta no pueda influir directamente en dicha operación de tratamiento de datos.

3. Cuál es el alcance de la expresión "interés legítimo", según la ponderación que debe realizarse conforme al artículo 7, letra f), de la Directiva 95/46/CE, en el sentido de si se refiere al interés en la inserción de contenidos de terceros o al interés del tercero.

4. A quién debe darse el consentimiento con arreglo a los artículos 7, letra a), y 2, letra h), de la Directiva 95/46/CE. Determinando también quién debe cumplir con la obligación de información que establece el artículo 10 de la señalada Directiva, el operador de la

[290] "Sin perjuicio del recurso administrativo que pueda interponerse, en particular ante la autoridad de control mencionada en el artículo 28, y antes de acudir a la autoridad judicial, los Estados miembros establecerán que toda persona disponga de un recurso judicial en caso de violación de los derechos que le garanticen las disposiciones de Derecho nacional aplicables al tratamiento de que se trate".

[291] "Los Estados miembros adoptarán las medidas adecuadas para garantizar la plena aplicación de las disposiciones de la presente Directiva y determinarán, en particular, las sanciones que deben aplicarse en caso de incumplimiento de las disposiciones adoptadas en ejecución de la presente Directiva".

[292] Es importante considerar que el artículo 80, apartado 2, del Reglamento 2016/679, que derogó y sustituyó la Directiva 95/46, autoriza expresamente el ejercicio de acciones judiciales por este tipo de asociaciones.

página web que ha insertado el contenido de un tercero, *Fashion ID*, o Facebook *Ireland*.

Sobre la primera cuestión planteada

Sobre el reconocimiento o no de las asociaciones de utilidad pública, para reclamar sobre las infracciones en materia de protección de datos que afecten a una persona física, el TJUE, señala que si bien el artículo 22 de la citada Directiva obliga a los Estados miembros a establecer que toda persona disponga de un recurso judicial en caso de violación de los derechos que le garanticen las disposiciones del Derecho nacional aplicables al tratamiento de datos personales, dicha Directiva no establece ninguna disposición que regule específicamente los requisitos del ejercicio de dicho recurso judicial[293]. Además, el artículo 24 de la Directiva 95/46/CE dispone que los Estados miembros adoptarán las "medidas adecuadas" para garantizar la plena aplicación de las disposiciones de esta Directiva, sin definir tales medidas.

Por consiguiente, el hecho de establecer la posibilidad de que una asociación de defensa de los intereses de los consumidores ejercite una acción judicial contra el presunto infractor de la protección de los datos personales, dice el TJUE, constituiría una medida adecuada.

El Tribunal señala además, que el hecho de que el RGPD (Reglamento 2016/679, que derogó y sustituyó la Directiva 95/46), autorice expresamente, en su artículo 80, apartado 2[294], a los Estados miembros a permitir que las asociaciones de defensa de los intereses de los consumidores ejerciten acciones judiciales contra el presunto infractor de la protección de los datos personales no implica en absoluto que los Estados miembros no pudieran conferirles ese derecho durante la vigencia de la Directiva 95/46/CE, sino que confirma, por el contrario, que la interpretación que de esta se ofrece en la sentencia refleja la voluntad del legislador de la Unión.

Sobre la segunda de las cuestiones planteadas

En otra de las cuestiones prejudiciales controvertidas, el órgano jurisdiccional remitente pregunta, en esencia, si el administrador de un sitio de Internet, como *Fashion ID*, que inserta en dicho sitio un módulo social que permite que el navegador del visitante de ese sitio solicite contenidos del proveedor de dicho módulo y transmita para ello a ese proveedor datos personales del visitante, puede ser considerado responsable del tratamiento, en el sentido del artículo 2, letra d), de la Directiva 95/46/CE, teniendo en cuenta que dicho administrador no tiene influencia alguna en el tratamiento de los datos transmitidos de ese modo al referido proveedor.

---

[293] Ver en este sentido, la sentencia de 27 de septiembre de 2017, *Puškár*, C-73/16, EU:C:2017:725, apartados 54 y 55.

[294] "Cualquier Estado miembro [podrá] disponer que cualquier entidad, organización o asociación mencionada en el apartado 1 del presente artículo tenga, con independencia del mandato del interesado, derecho a presentar en ese Estado miembro una reclamación ante la autoridad de control que sea competente en virtud del artículo 77 y a ejercer los derechos contemplados en los artículos 78 y 79, si considera que los derechos del interesado con arreglo al presente Reglamento han sido vulnerados como consecuencia de un tratamiento".

Para abordar esta controversia, el TJUE señala, como ya ha dado cuenta su propia jurisprudencia[295], que hay que considerar que tal como establece expresamente el artículo 2, letra d), de la Directiva 95/46/CE, el concepto de "responsable del tratamiento" se refiere al organismo que "solo o conjuntamente con otros" determine los fines y los medios del tratamiento de datos personales, y que dicho concepto no se refiere necesariamente a un único organismo, sino que puede aludir a varios agentes que participen en ese tratamiento, cada uno de los cuales estará sujeto, por lo tanto, a las disposiciones aplicables en materia de protección de datos.

Así las cosas, dado que el objetivo del artículo 2, letra d), de la Directiva 95/46/CE consiste en garantizar, mediante una definición amplia el concepto de "responsable", la responsabilidad conjunta no significa que, sobre un mismo tratamiento de datos personales, los diversos agentes tengan una responsabilidad equivalente. Por el contrario, los agentes pueden estar implicados en distintas etapas del tratamiento y en distintos grados, de modo que el nivel de responsabilidad de cada uno de ellos debe evaluarse teniendo en cuenta todas las circunstancias pertinentes del caso concreto. Tal como se analizó hace algunas líneas atrás en la sentencia del TJUE de 10 de julio de 2018, *Jehovan todistajat*, C-25/17[296].

Además, el Tribunal declara que al insertar el módulo social "me gusta" en su sitio de Internet, *Fashion ID* influye de manera decisiva en la recogida y transmisión de datos personales de los visitantes de ese sitio a favor del proveedor de ese módulo, en este caso Facebook *Ireland*, en términos tales que, de no haberse insertado ese módulo, no se habrían recogido ni transmitido tales datos. Por lo que considera que Facebook *Ireland* y *Fashion ID* determinan conjuntamente los medios que originan las operaciones de recogida y de comunicación por transmisión de datos personales de los visitantes del sitio de Internet de *Fashion ID*. En consecuencia, dice el Tribunal, *Fashion ID* puede ser considerada responsable, en el sentido del artículo 2, letra d), de la Directiva 95/46/CE, conjuntamente con Facebook *Ireland*, de las operaciones de recogida y de comunicación por transmisión de datos personales de los visitantes de su sitio de Internet.

Sobre la tercera cuestión planteada

Sobre la cuestión prejudicial relacionada con el interés legítimo, el órgano jurisdiccional remitente pregunta al TJUE, si el administrador de un sitio de Internet inserta en dicho sitio un módulo social que permite que el navegador del visitante de ese sitio solicite contenidos del proveedor de dicho módulo y transmita para ello a ese proveedor datos personales del visitante, es preciso tener en cuenta, a efectos de la aplicación del artículo 7, letra f), de la Directiva 95/467CE[297], el interés legítimo perseguido por dicho administrador o el interés legítimo perseguido por el proveedor.

---

[295] Ver en este sentido, las sentencias de 5 de junio de 2018, *Wirtschaftsakademie Schleswig-Holstein*, C-210/16, EU: C: 2018:388, apartado 29, y de 10 de julio de 2018, *Jehovan todistajat*, C-25/17, EU:C:2018:551, apartado 65.

[296] Apartado 66.

[297] "Los Estados miembros dispondrán que el tratamiento de datos personales solo pueda efectuarse si: f) es necesario para la satisfacción del interés legítimo perseguido por el responsable del tratamiento o por el tercero o terceros a los que se comuniquen los datos, siempre que no prevalezca el interés o los derechos y libertades

A este respecto, el Tribunal establece que, según lo dispuesto en el capítulo II de la Directiva 95/46/CE, titulado "Condiciones generales para la licitud del tratamiento de datos personales", todo tratamiento de datos personales debe ser conforme, en particular, con alguno de los principios relativos a la legitimación del tratamiento de datos enumerados en el artículo 7 de la citada Directiva[298].

Por lo tanto, el señalado artículo 7, letra f), establece tres requisitos acumulativos para que un tratamiento de datos personales sea lícito, a saber: en primer lugar, que el responsable del tratamiento o el tercero o terceros a los que se comuniquen los datos persigan un interés legítimo; en segundo lugar, la necesidad del tratamiento de datos personales para la satisfacción del interés legítimo perseguido; y, en tercer lugar, el requisito de que no prevalezcan los derechos y libertades fundamentales del interesado.

Así entonces, resuelve el TJUE, cuando el administrador de un sitio de Internet, en este caso *Fashion ID* inserta en dicho sitio un módulo social que permite que el navegador del visitante de ese sitio solicite contenidos del proveedor de dicho módulo, en la especie Facebook Ireland y transmita para ello a ese proveedor datos personales del visitante, puede ser considerado responsable de las operaciones de tratamiento de datos personales de los visitantes de su sitio de Internet que son la recogida y la comunicación por transmisión, siendo necesario que cada uno de esos responsables persiga, con tales operaciones de tratamiento, un interés legítimo, en el sentido del artículo 7, letra f), de la Directiva 95/46/CE, para que estas queden justificadas.

Sobre la cuarta cuestión planteada

Finalmente, el órgano jurisdiccional remitente consulta al TJUE, por un lado, si los artículos 2 letra h)[299] y 7 letra a)[300] de la Directiva 95/46/CE, deben interpretarse en el sentido que en una situación como la controvertida, donde el administrador de un sitio de Internet inserta en dicho sitio un módulo social que permite que el navegador del visitante de ese sitio solicite contenidos del proveedor de dicho módulo y transmita para ello a ese proveedor datos personales de dicho visitante, el consentimiento mencionado en tales disposiciones debe ser solicitado por el administrador o por el proveedor y, por otro lado, si el artículo 10 de la citada Directiva debe interpretarse en el sentido de que, en tal situación, la obligación de información establecida en esa disposición recae sobre dicho administrador.

> *Artículo 10 Directiva 95/46/CE; "Información en caso de obtención de datos recabados del propio interesado los Estados miembros dispondrán que el responsable del tratamiento o su representante deberán comunicar a la persona de quien se recaben los datos que le conciernan, por lo menos la información que se enumera a continuación, salvo si la persona ya hubiera sido informada de ello: a) la identidad del responsable del tratamiento y, en su caso, de su representante; b) los fines del*

fundamentales del interesado que requieran protección con arreglo al apartado 1 del artículo 1 de la presente Directiva".

[298] Ver en este sentido, las sentencias de 13 de mayo de 2014, Google Spain y Google, C-131/12, EU:C:2014:317, apartado 71, y de 1 de octubre de 2015, Bara y otros, C-201/14, EU:C:2015:638, apartado 30.

[299] "consentimiento del interesado: toda manifestación de voluntad, libre, específica e informada, mediante la que el interesado consienta el tratamiento de datos personales que le conciernan".

[300] "el interesado ha dado su consentimiento de forma inequívoca".

> *tratamiento de que van a ser objeto los datos; c) cualquier otra información tal como: - los destinatarios o las categorías de destinatarios de los datos, - el carácter obligatorio o no de la respuesta y las consecuencias que tendría para la persona interesada una negativa a responder, - la existencia de derechos de acceso y rectificación de los datos que la conciernen, en la medida en que, habida cuenta de las circunstancias específicas en que se obtengan los datos, dicha información suplementaria resulte necesaria para garantizar un tratamiento de datos leal respecto del interesado."*

Como ya se señaló, el TJUE determinó que el administrador de un sitio de Internet, en este caso *Fashion ID*, puede ser considerado responsable del tratamiento de datos de carácter personal, responsabilidad que se limita a la operación o al conjunto de las operaciones de tratamiento de datos personales cuyos fines y medios determina efectivamente.

Así pues, resulta que las obligaciones que pueden incumbir, conforme a la Directiva 95/46/CE, a ese responsable del tratamiento, como la obligación de solicitar el consentimiento del interesado mencionado en los artículos 2, letra h), y 7, letra a), de dicha Directiva, y la obligación de información establecida en el artículo 10 de esta, deben referirse a la operación o al conjunto de las operaciones de tratamiento de datos personales cuyos fines y medios determina efectivamente.

En el caso en análisis , si bien *Fashion ID,* como administrador de un sitio de Internet que inserta en dicho sitio un módulo social, permite que el navegador del visitante de ese sitio solicite contenidos del proveedor (Facebook *Ireland*) de dicho módulo y transmita para ello a ese proveedor datos personales del visitante, puede ser considerado responsable conjuntamente con ese proveedor de las operaciones de recogida y de comunicación por transmisión de datos personales de dicho visitante, su obligación de solicitar el consentimiento del interesado, mencionado en los artículos 2, letra h), y 7, letra a), de la Directiva 95/46/CE, y su obligación de información establecida en el artículo 10 de esta se refieren únicamente a esas operaciones. En cambio, dichas obligaciones no se extienden a las operaciones de tratamiento de datos personales relativas a las demás fases, anteriores o posteriores a dichas operaciones, que impliquen, en su caso, el tratamiento de datos personales en cuestión.

Este consentimiento debe darse con anterioridad a la recogida y a la comunicación por transmisión de datos del interesado. En estas circunstancias, incumbe al administrador del sitio de Internet *Fashion ID*, y no al proveedor del módulo social, solicitar dicho consentimiento, en la medida en que es el hecho de que un visitante consulte ese sitio de Internet lo que desencadena el proceso de tratamiento de datos personales. Eso sí, el consentimiento que debe prestarse al administrador se refiere únicamente a la operación o al conjunto de las operaciones de tratamiento de datos personales cuyos fines y medios determina efectivamente dicho administrado.

En lo que respecta al deber de información establecido en el artículo 10 de la Directiva 95/46/CE, se desprende que el responsable del tratamiento o su representante deben comunicar a la persona de quien se recaben los datos por lo menos la información mencionada en la citada disposición. Por lo tanto, resulta que el responsable del tratamiento, en este caso *Fashion ID*, debe dar dicha información inmediatamente, a saber, en el momento en el que se recaban los

datos[301], referida únicamente a la operación o al conjunto de las operaciones de tratamiento de datos personales cuyos fines y medios determina efectivamente dicho administrador.

Sentencia C-136/17- GC y otros, de 24 de septiembre de 2019

A continuación se encuentra la sentencia C-136/17- GC y otros (*Déréférencement de données sensibles*), Sentencia del Tribunal de Justicia (Gran Sala) de 24 de septiembre de 2019, GC y otros contra *Commission nationale de l'informatique et des libertés* (CNIL), cuyos antecedentes en general se refieren a información alojada en el motor de búsqueda Google, en que los solicitantes requieren su retiro, frente a la negativa de Google, se dirigen ante la autoridad francesa, la *Commission nationale de l'informatique et des libertés* (CNIL), que archiva los antecedentes, ante lo cual los afectados recurren ante el *Conseil d'État* (Consejo de Estado francés como Tribunal Supremo de lo Contencioso-Administrativo), el cual es el órgano que remite los antecedentes al TJUE. Las alegaciones de los afectados, que se individualizan con sus respectivas iniciales, pueden resumirse de la siguiente manera:

GC había solicitado la retirada de un enlace que remitía a un fotomontaje satírico publicado en línea, bajo seudónimo, el 18 de febrero de 2011 en el canal YouTube, en el que se la representaba junto al alcalde de un municipio del que era jefa de gabinete y se comentaba de forma explícita la relación íntima que supuestamente mantenía con él y el efecto que esa relación había tenido en su propia proyección política. El referido fotomontaje fue publicado en Internet con ocasión de la campaña electoral para las elecciones cantonales en las que GC se había presentado como candidata. En la fecha en que se denegó la solicitud de retirada de enlaces presentada por la interesada, esta no había sido elegida ni era candidata a ningún cargo político local y ya no ejercía las funciones de jefa de gabinete del alcalde del referido municipio.

AF había solicitado la retirada de enlaces que remitían a un artículo del diario *Libération* de 9 de septiembre de 2008, reproducido en el sitio de Internet del *Centre contre les manipulations mentales* (CCMM) (Centro contra la Manipulación Mental de Francia), relativo al suicidio de una adepta de la Iglesia de la Cienciología en diciembre de 2006. En dicho artículo, se mencionaba a AF como responsable de relaciones públicas de la Iglesia de la Cienciología, función que ya no ejercía, Además, el autor de dicho artículo afirmaba que se había puesto en contacto con AF para obtener su versión de los hechos y relataba las declaraciones recabadas en ese contexto.

BH había solicitado la retirada de enlaces que remitían a artículos, fundamentalmente periodísticos, sobre un sumario abierto en el mes de junio de 1995 en relación con la financiación del *Parti Républicain* (PR), en el marco del cual fue investigado junto con varios empresarios y políticos. El procedimiento incoado en su contra concluyó mediante auto de sobreseimiento de 26 de febrero de 2010. La mayor parte de los enlaces controvertidos dirigían

[301] Ver en este sentido, las sentencias de 7 de mayo de 2009, *Rijkeboer*, C-553/07, EU:C:2009:293, apartado 68, y de 7 de noviembre de 2013, IPI, C-473/12, EU:C:2013:715, apartado 23.

a artículos que se habían publicado en el momento en que se inició la fase de instrucción, por lo que no informaban del desenlace del procedimiento.

ED había solicitado la retirada de enlaces que remitían a dos artículos, publicados por los diarios *Nice Matin* y *Le Figaro*, en los que se informaba del juicio oral en el que ED fue condenado a una pena de siete años de prisión y a una pena accesoria de diez años de seguimiento socio-judicial por agresión sexual a menores de quince años. Una de estas crónicas judiciales mencionaba, además, varios detalles íntimos relativos a ED, que salieron a la luz durante el juicio.

Tras ver denegadas sus solicitudes de retirada de enlaces por parte de Google, los demandantes en el litigio principal presentaron denuncias ante la CNIL para que se instara a dicha sociedad a retirar los enlaces controvertidos. Mediante respectivos escritos de 24 de abril de 2015, 28 de agosto de 2015, 21 de marzo de 2016 y 9 de mayo de 2016, la Presidenta de la CNIL informó a los demandantes en el litigio principal de que sus denuncias habían sido archivadas.

Frente a la respuesta del CNIL, los demandantes interpusieron ante el órgano jurisdiccional remitente, el *Conseil d'État* Consejo de Estado, recursos contra las negativas de la CNIL de requerir a Google que retirara los enlaces señalados, ante lo cual el *Conseil d'État* acumulo estos recursos y procedió a suspender el procedimiento remitiendo los antecedentes al TJUE, planteando en síntesis las siguientes cuestiones prejudiciales[302]:

1. Determinar si al gestor de un motor de búsqueda, en este caso Google, le son aplicables las disposiciones relacionadas con la prohibición del tratamiento de datos de carácter personal, previstas en los apartados 1 y 5 del artículo 8 de la Directiva 95/46/CE, con sus respectivas excepciones. Si esta determinación es afirmativa ¿Google está obligado a acoger las solicitudes para retirar los enlaces que direccionen a páginas web donde se traten datos de los afectados?

2. ¿Puede negarse dicho gestor a aceptar una solicitud de retirada cuando constate que los enlaces controvertidos dirigen a contenido que, si bien incluye datos comprendidos en las categorías mencionadas en el apartado 1 del artículo 8, de la Directiva 95/46/CE, está igualmente comprendido en el ámbito de aplicación de las excepciones previstas en el apartado 2 de este mismo artículo, en concreto, en sus letras a) y e)?

3. Procede el retiro de los enlaces o direccionamiento a páginas web, cuando estos conducen a tratamientos de datos personales efectuados con fines exclusivamente periodísticos o de expresión artística o literaria, los cuales pueden, por ese motivo, en

[302] Es importante considerar que las cuestiones prejudiciales planteadas tienen por objeto la interpretación de la Directiva 95/46/CE, que era aplicable en la fecha de presentación de la petición de decisión, sin embargo, esta Directiva fue derogada el 25 de mayo de 2018, fecha a partir de la cual se aplica el Reglamento 2016/679 RGPD. El TJUE examina las cuestiones prejudiciales planteadas a la luz de la Directiva, pero igualmente para el análisis, tiene en consideración el RGPD con el fin de garantizar que sus respuestas sean útiles para el órgano jurisdiccional remitente.

virtud del artículo 9 de la Directiva 95/46/CE, recoger y tratar datos comprendidos en las categorías mencionadas en el artículo 8, apartados 1 y 5, de esta Directiva.

4. Cuando el solicitante demuestre que, habida cuenta del desarrollo de un procedimiento judicial, la información relativa a una etapa anterior de ese procedimiento ya no se corresponde con la realidad de su situación, ¿está obligado el gestor de un motor de búsqueda a retirar los enlaces que dirijan a las páginas web que contienen tal información?

5. ¿Debe interpretarse el artículo 8, apartado 5, de la Directiva 95/46/CE en el sentido de que los datos sobre la imputación de una persona o sobre un juicio, y la condena que se deriva de este, constituyen datos relativos a infracciones y a condenas penales? En general, cuando una página web contiene datos sobre la condena o los procedimientos judiciales que atañen a una persona física, ¿está comprendida esa página web en el ámbito de aplicación de esta disposición?

Sobre la primera cuestión planteada

La primera cuestión prejudicial planteada por el órgano remitente persigue determinar si el artículo 8, apartados 1[303] y 5[304], de la Directiva 95/46/CE, deben interpretarse en el sentido de que la prohibición o las restricciones relativas al tratamiento de las categorías especiales de datos personales a las que se refiere, se aplican, sin perjuicio de las excepciones establecidas en esa Directiva, al gestor de un motor de búsqueda, en este caso a Google.

En este sentido, es importante recordar que la actividad de un motor de búsqueda consiste en hallar información publicada o puesta en Internet por terceros, indexarla de manera automática, almacenarla temporalmente y ponerla a disposición de los internautas según un orden de preferencia determinado. Para el TJUE toda esta actividad debe calificarse de "tratamiento de datos personales", en el sentido del artículo 2, letra b), de la Directiva 95/46/CE, cuando esa información contenga datos personales y por consiguiente el gestor de un motor de búsqueda, agrega dicho Tribunal, debe ser considerado "responsable" del tratamiento, en el sentido del artículo 2, letra d), de esa Directiva[305].

Conviene también considerar que el contenido del artículo 8, apartados 1 y 5, en análisis, ha quedado recogido también, con algunas modificaciones, en los artículos 9, apartado 1 y 10 del Reglamento 2016/679.

---

[303] "Los Estados miembros prohibirán el tratamiento de datos personales que revelen el origen racial o étnico, las opiniones políticas, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, así como el tratamiento de los datos relativos a la salud o a la sexualidad".

[304] "El tratamiento de datos relativos a infracciones, condenas penales o medidas de seguridad solo podrá efectuarse bajo el control de la autoridad pública o si hay previstas garantías específicas en el Derecho nacional, sin perjuicio de las excepciones que podrá establecer el Estado miembro basándose en disposiciones nacionales que prevean garantías apropiadas y específicas. Sin embargo, solo podrá llevarse un registro completo de condenas penales bajo el control de los poderes públicos".

[305] Ver sentencia de 13 de mayo de 2014, Google Spain y Google, C-131/12, EU:C:2014:317, apartado 41.

> *Artículo 9, apartado 1 del RGPD; "Quedan prohibidos el tratamiento de datos personales que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, y el tratamiento de datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud o datos relativos a la vida sexual o las orientaciones sexuales de una persona física".*

> *Artículo 9, apartado 10 del RGPD; "El tratamiento de datos personales relativos a condenas e infracciones penales o medidas de seguridad conexas sobre la base del artículo 6, apartado 1, sólo podrá llevarse a cabo bajo la supervisión de las autoridades públicas o cuando lo autorice el Derecho de la Unión o de los Estados miembros que establezca garantías adecuadas para los derechos y libertades de los interesados. Solo podrá llevarse un registro completo de condenas penales bajo el control de las autoridades públicas".*

En este sentido, de las señaladas disposiciones tanto de la Directiva como del RGPD se desprende que la prohibición y las restricciones que establecen se aplican, sin perjuicio de las excepciones previstas, a todos los tratamientos de las categorías especiales de datos a las que se refieren y a todos los responsables que realicen tales tratamientos.

El TJUE agrega que, excluir *a priori* y de forma general la actividad de un motor de búsqueda de las exigencias específicas que estas disposiciones establecen en relación con los tratamientos de las categorías especiales de datos a las que se refieren, sería contraria a la finalidad de dichas disposiciones, que buscan garantizar una mayor protección frente a tales tratamientos que, en atención a la particular sensibilidad de esos datos, pueden constituir, como se desprende igualmente del considerando 33 de la Directiva y del considerando 51 del Reglamento, una injerencia especialmente grave en los derechos fundamentales al respeto de la vida privada y a la protección de los datos personales, garantizados por los artículos 7 y 8 de la CDFUE.

> *Considerando 33 de la Directiva 96/46/CE; "Considerando, por lo demás , que los datos que por su naturaleza puedan atentar contra las libertades fundamentales o la intimidad no deben ser objeto de tratamiento alguno, salvo en caso de que el interesado haya dado su consentimiento explícito; que deberán constar de forma explícita las excepciones a esta prohibición para necesidades específicas, en particular cuando el tratamiento de dichos datos se realice con fines relacionados con la salud, por parte de personas físicas sometidas a una obligación legal de secreto profesional, o para actividades legítimas por parte de ciertas asociaciones o fundaciones cuyo objetivo sea hacer posible el ejercicio de libertades fundamentales".*

> *Considerando 51 del RGPD; "Especial protección merecen los datos personales que, por su naturaleza, son particularmente sensibles en relación con los derechos y las libertades fundamentales, ya que el contexto de su tratamiento podría entrañar importantes riesgos para los derechos y las libertades fundamentales. Debe incluirse entre tales datos personales los datos de carácter personal que revelen el origen racial o étnico, entendiéndose que el uso del término «origen racial» en el presente Reglamento no implica la aceptación por parte de la Unión de teorías que traten de determinar la existencia de razas humanas separadas. El tratamiento de fotografías*

> *no debe considerarse sistemáticamente tratamiento de categorías especiales de datos personales, pues únicamente se encuentran comprendidas en la definición de datos biométricos cuando el hecho de ser tratadas con medios técnicos específicos permita la identificación o la autenticación unívocas de una persona física. Tales datos personales no deben ser tratados, a menos que se permita su tratamiento en situaciones específicas contempladas en el presente Reglamento, habida cuenta de que los Estados miembros pueden establecer disposiciones específicas sobre protección de datos con objeto de adaptar la aplicación de las normas del presente Reglamento al cumplimiento de una obligación legal o al cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento. Además de los requisitos específicos de ese tratamiento, deben aplicarse los principios generales y otras normas del presente Reglamento, sobre todo en lo que se refiere a las condiciones de licitud del tratamiento. Se deben establecer de forma explícita excepciones a la prohibición general de tratamiento de esas categorías especiales de datos personales, entre otras cosas cuando el interesado dé su consentimiento explícito o tratándose de necesidades específicas, en particular cuando el tratamiento sea realizado en el marco de actividades legítimas por determinadas asociaciones o fundaciones cuyo objetivo sea permitir el ejercicio de las libertades fundamentales"*.

De las anteriores consideraciones, el TJUE concluye sobre la cuestión prejudicial que se le formula que, al gestor de un motor de búsqueda, en este caso Google, sí le son aplicables las disposiciones relacionadas con la prohibición del tratamiento de datos de carácter personal, previstas en los apartados 1 y 5 del artículo 8 de la Directiva 95/46/CE, con sus respectivas excepciones.

En este sentido, como subraya la Comisión Europea, el gestor de un motor de búsqueda no es responsable de que los datos personales a los que se refieren dichas disposiciones figuren en una página web publicada por un tercero, sino de crear un enlace a esa página y, sobre todo, de mostrarlo en la lista de resultados que se presenta a los internautas tras una búsqueda efectuada a partir del nombre de una persona física, ya que mostrar tal enlace puede afectar significativamente a los derechos fundamentales del interesado respeto de su vida privada y a la protección de los datos personales que le conciernen[306].

Sobre la segunda y tercera de las cuestiones planteadas

Ahora bien, sobre si Google, como gestor de un motor de búsqueda, está obligado, sin perjuicio de las excepciones establecidas en la Directiva, a acoger las solicitudes de retirada de enlaces que dirigen a páginas web en las que figuran datos personales comprendidos en las categorías especiales. El TJUE señala que hay que distinguir y considerar diversas situaciones previstas en las disposiciones tanto de la Directiva 95/46/CE, como del RGPD y la CDFUE.

En efecto, las solicitudes de retirada de enlaces como las controvertidas en el caso en análisis, tienen su fundamento en el artículo 12, letra b) y en el artículo 14, párrafo primero, letra a) de la Directiva 95/46/CE. En el artículo 12 letra b) se establece que los Estados miembros

[306] Ver sentencia de 13 de mayo de 2014, Google *Spain* y Google, C-131/12, EU:C:2014:317, apartado 80.

garantizarán a los interesados el derecho de obtener del responsable del tratamiento la supresión de los datos cuyo tratamiento no se ajuste a las disposiciones de la misma; y en el artículo 14, párrafo primero, letra a), se dispone que los Estados miembros reconocerán al interesado el derecho a oponerse, al menos en los casos contemplados en el artículo 7, letras e)[307] y f)[308], de la Directiva 95/46/CE, en cualquier momento y por razones legítimas propias de su situación particular, a que los datos que le conciernan sean objeto de tratamiento, salvo cuando la legislación nacional disponga otra cosa.

A este respecto, es preciso recordar que el Tribunal de Justicia ha declarado que los artículos 12, letra b), y 14, párrafo primero, letra a), de la Directiva 95/46/CE deben interpretarse en el sentido que, para respetar los derechos que establecen estas disposiciones, el gestor de un motor de búsqueda está obligado a eliminar de la lista de resultados obtenida tras una búsqueda efectuada a partir del nombre de una persona enlaces a páginas web, publicadas por terceros y que contienen información relativa a esta persona, también en el supuesto de que este nombre o esta información no se borre previa o simultáneamente de estas páginas web, y, en su caso, aunque la publicación en dichas páginas sea en sí misma lícita[309].

El TJUE también sostiene que se deben tener en cuenta las disposiciones contenidas en la CDFUE, considerando los derechos que se reconocen en los artículos 7[310] (respeto de la vida privada y familiar) y 8[311] (protección de datos de carácter personal) , por cuanto estos derechos prevalecen, en principio, no solo sobre el interés económico del gestor del motor de búsqueda, sino también sobre el interés del público en acceder a dicha información, en una búsqueda que tenga por objeto el nombre de esa persona. El Tribunal recuerda eso sí, que, si el interesado ha desempeñado un papel en la vida pública, la injerencia en sus derechos fundamentales está justificada por el interés preponderante del público en tener, a raíz de esta inclusión, acceso a la información de que se trate[312].

Similar regulación se encuentra en el RGPD, que en su artículo 17 consagra el derecho a supresión, también denominado "derecho al olvido". En su apartado 1 se establece que el interesado tendrá derecho a obtener sin dilación indebida del responsable del tratamiento la supresión de los datos personales que le conciernan, estando el responsable del tratamiento obligado a suprimir lo antes posible esos datos cuando concurra alguna de las circunstancias

---

[307] "es necesario para el cumplimiento de una misión de interés público o inherente al ejercicio del poder público conferido al responsable del tratamiento o a un tercero a quien se comuniquen los datos".

[308] "es necesario para la satisfacción del interés legítimo perseguido por el responsable del tratamiento o por el tercero o terceros a los que se comuniquen los datos, siempre que no prevalezca el interés o los derechos y libertades fundamentales del interesado que requieran protección con arreglo al apartado 1 del artículo 1 de la presente Directiva".

[309] Ver sentencia de 13 de mayo de 2014, Google *Spain* y Google, C-131/12, EU:C:2014:317, apartado 88.

[310] "Respeto de la vida privada y familiar: Toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de sus comunicaciones".

[311] "Protección de datos de carácter personal; 1. Toda persona tiene derecho a la protección de los datos de carácter personal que la conciernan. 2. Estos datos se tratarán de modo leal, para fines concretos y sobre la base del consentimiento de la persona afectada o en virtud de otro fundamento legítimo previsto por la ley. Toda persona tiene derecho a acceder a los datos recogidos que la conciernan y a obtener su rectificación". 3. El respeto de estas normas estará sujeto al control de una autoridad independiente".

[312] Ver sentencia de 13 de mayo de 2014, Google *Spain* y Google, C-131/12, EU:C:2014:317, apartado 99.

enumeradas en esta disposición, las cuales son: el hecho que los datos ya no sean necesarios en relación con los fines para los que fueron tratados; que el interesado retire el consentimiento en que se basa el tratamiento y tal tratamiento no se base en otro fundamento jurídico; que el interesado se oponga al tratamiento con arreglo al artículo 21, apartados 1 o 2[313], de este Reglamento, que los datos hayan sido tratados ilícitamente; que estos deban suprimirse para cumplir una obligación legal, o que se hayan obtenido en relación con la oferta a niños de servicios de la sociedad de la información.

> *Artículo 21, apartado 1 RGPD; "El interesado tendrá derecho a oponerse en cualquier momento, por motivos relacionados con su situación particular, a que datos personales que le conciernan sean objeto de un tratamiento basado en lo dispuesto en el artículo 6, apartado 1, letras e) o f), incluida la elaboración de perfiles sobre la base de dichas disposiciones. El responsable del tratamiento dejará de tratar los datos personales, salvo que acredite motivos legítimos imperiosos para el tratamiento que prevalezcan sobre los intereses, los derechos y las libertades del interesado, o para la formulación, el ejercicio o la defensa de reclamaciones".*

> *Artículo 21, apartado 2 RGPD; "Cuando el tratamiento de datos personales tenga por objeto la mercadotecnia directa, el interesado tendrá derecho a oponerse en todo momento al tratamiento de los datos personales que le conciernan, incluida la elaboración de perfiles en la medida en que esté relacionada con la citada mercadotecnia".*

Sin embargo, el artículo 17, apartado 3, de dicho Reglamento especifica que el artículo 17 apartado 1, no se aplicará cuando el tratamiento sea necesario por alguna de las razones enunciadas entre las que se distinguen el ejercicio del derecho a la libertad de información. El hecho que el artículo 17, apartado 3, letra a), del Reglamento 2016/679 establezca ya expresamente que el derecho al olvido del interesado queda excluido cuando el tratamiento resulta necesario para ejercer, entre otros, el derecho a la libertad de información, garantizado por el artículo 11 de la Carta[314], pone de manifiesto que el derecho a la protección de los datos personales no constituye un derecho absoluto, sino que, como subraya el considerando 4 del RGPD, debe entenderse en relación con su función en la sociedad y mantener el equilibrio con otros derechos fundamentales, con arreglo al principio de proporcionalidad[315].

> *Considerando 4 RGPD; "El tratamiento de datos personales debe estar concebido para servir a la humanidad. El derecho a la protección de los datos personales no es un derecho absoluto, sino que debe considerarse en relación con su función en la sociedad y mantener el equilibrio con otros derechos fundamentales, con arreglo al*

---

[313] "Cuando el tratamiento de datos personales tenga por objeto la mercadotecnia directa, el interesado tendrá derecho a oponerse en todo momento al tratamiento de los datos personales que le conciernan, incluida la elaboración de perfiles en la medida en que esté relacionada con la citada mercadotecnia".

[314] "Libertad de expresión y de información: 1. Toda persona tiene derecho a la libertad de expresión. Este derecho comprende la libertad de opinión y la libertad de recibir o comunicar informaciones o ideas sin que pueda haber injerencia de autoridades públicas y sin consideración de fronteras; 2. Se respetan la libertad de los medios de comunicación y su pluralismo".

[315] Ver en este sentido, la sentencia de 9 de noviembre de 2010, *Volker und Markus Schecke* y *Eifert*, C-92/09 y C-93/09, EU:C:2010:662, apartado 48.

> *principio de proporcionalidad. El presente Reglamento respeta todos los derechos fundamentales y observa las libertades y los principios reconocidos en la Carta conforme se consagran en los Tratados, en particular el respeto de la vida privada y familiar, del domicilio y de las comunicaciones, la protección de los datos de carácter personal, la libertad de pensamiento, de conciencia y de religión, la libertad de expresión y de información, la libertad de empresa, el derecho a la tutela judicial efectiva y a un juicio justo, y la diversidad cultural, religiosa y lingüística"*.

En este contexto, cabe recordar que el artículo 52, apartado 1, de la Carta[316] reconoce que pueden introducirse limitaciones al ejercicio de derechos y libertades como los consagrados en los artículos 7 y 8 de esta, siempre que tales limitaciones estén establecidas por la Ley, respeten el contenido esencial de dichos derechos y libertades y el principio de proporcionalidad, sean necesarias y respondan efectivamente a objetivos de interés general reconocidos por la Unión o a la necesidad de protección de los derechos y libertades de los demás[317].

Teniendo en cuenta estas consideraciones, debe examinarse en qué situaciones el gestor de un motor de búsqueda está obligado a acoger una solicitud de retirada de enlaces y, por lo tanto, a suprimir de la lista de resultados obtenida el enlace a una página web en la que figuran datos personales comprendidos en las categorías especiales a las que se refiere el ya citado artículo 8, apartados 1 y 5, de la Directiva 95/46/CE. Y en qué situaciones de excepción, el gestor de un motor de búsqueda puede rechazar tales solicitudes de eliminación, cuestión que como se verá puede tener dos fundamentos: el consentimiento del interesado y que se trate de datos manifiestamente públicos.

En efecto, el artículo 8, apartado 2, letras a) y e) de la Directiva dispone que la prohibición de tratamiento de esas categorías especiales de datos no se aplicará cuando el interesado haya dado su consentimiento explícito[318] a dicho tratamiento, salvo en los casos en los que la legislación del Estado miembro de que se trate prohíba tal consentimiento, o cuando el tratamiento se refiera a datos que el interesado haya hecho manifiestamente públicos.

En la práctica, es difícilmente concebible, y por lo demás no se desprende del caso en análisis, que el gestor de un motor de búsqueda (Google) solicite el consentimiento expreso de los interesados antes de tratar, a efectos de su actividad de enumeración de resultados, los datos personales que conciernen a aquellos. En cualquier caso, el hecho mismo de que una persona presente una solicitud de retirada de enlaces significa, en principio, que al menos en la fecha

---

[316] "Cualquier limitación del ejercicio de los derechos y libertades reconocidos por la presente Carta deberá ser establecida por la ley y respetar el contenido esencial de dichos derechos y libertades. Dentro del respeto del principio de proporcionalidad, sólo podrán introducirse limitaciones cuando sean necesarias y respondan efectivamente a objetivos de interés general reconocidos por la Unión o a la necesidad de protección de los derechos y libertades de los demás".

[317] Ver sentencia de 9 de noviembre de 2010, *Volker und Markus Schecke* y Eifert, C-92/09 y C-93/09, EU:C:2010:662, apartado 50.

[318] La expresión "consentimiento", regulada tanto en la Directiva 95/46/CE como en el RGPD, hay que entenderla con una característica consustancial, cual es que ese consentimiento debe ser "específico" y, por lo tanto, referirse concretamente al tratamiento realizado en el marco de la actividad del motor de búsqueda; en consecuencia, al hecho de que el tratamiento permite a terceros obtener, mediante una búsqueda efectuada a partir del nombre del interesado, una lista de resultados que incluye enlaces que dirigen a páginas web que contienen datos sensibles que le conciernen.

de dicha solicitud, ya no consiente en el tratamiento que realiza el gestor del motor de búsqueda[319].

La otra excepción contenida en el artículo 8, apartado 2, letra e), de la Directiva 95/46/CE y en el artículo 9, apartado 2, letra e), del Reglamento 2016/679, relativa a que el interesado haya hecho manifiestamente públicos los datos de que se trate, se aplica tanto al gestor del motor de búsqueda (Google) como al editor de la página web en cuestión. Sin embrago, aún en ese caso el interesado puede tener derecho a que se retire el enlace controvertido por razones propias de su situación particular[320].

En todo caso, el gestor de un motor de búsqueda que reciba una solicitud de retirada de enlaces deberá comprobar, a la luz de los motivos de interés público imperantes a los que se refieren el artículo 8, apartado 4, de la Directiva 95/46/CE y el artículo 9, apartado 2, letra g), del Reglamento 2016/679 y respetando los requisitos establecidos en estas disposiciones, si la inclusión del enlace que dirige a la página web en cuestión, en la lista de resultados obtenida tras una búsqueda efectuada a partir del nombre del interesado, es necesaria para el ejercicio del derecho a la libertad de información de los internautas potencialmente interesados en acceder a esa página web mediante tal búsqueda, libertad garantizada por el artículo 11 de la Carta.

Aunque los derechos del interesado protegidos por los artículos 7 y 8 de la Carta prevalecen, con carácter general, sobre la libertad de información de los internautas, este equilibrio puede depender, en supuestos específicos, de la naturaleza de la información de que se trate, del carácter sensible de esta para la vida privada del interesado y del interés del público en disponer de esta información, que puede variar, en particular, en función del papel que el interesado desempeñe en la vida pública[321].

Del conjunto de consideraciones anteriores, el TJUE se pronuncia sobre estas cuestiones prejudiciales señalando:

a) El gestor de un motor de búsqueda está obligado, en principio, sin perjuicio de las excepciones establecidas en la Directiva 95/46/CE, a acoger las solicitudes de retirada de enlaces que dirigen a páginas web en las que figuran datos personales comprendidos en las categorías especiales.

---

[319] El artículo 17, apartado 1, letra b), del RGPD contempla, entre las circunstancias que justifican el derecho al olvido, el que el interesado retire el consentimiento en que se basa el tratamiento de conformidad con el artículo 9, apartado 2, letra a), del mismo Reglamento y que tal tratamiento no se base en otro fundamento jurídico.

[320] El artículo 21, aparatado 1 del RGPD, dispone: "El interesado tendrá derecho a oponerse en cualquier momento, por motivos relacionados con su situación particular, a que datos personales que le conciernan sean objeto de un tratamiento basado en lo dispuesto en el artículo 6, apartado 1, letras e) o f), incluida la elaboración de perfiles sobre la base de dichas disposiciones. El responsable del tratamiento dejará de tratar los datos personales, salvo que acredite motivos legítimos imperiosos para el tratamiento que prevalezcan sobre los intereses, los derechos y las libertades del interesado, o para la formulación, el ejercicio o la defensa de reclamaciones".

[321] Ver en este sentido, la sentencia de 13 de mayo de 2014, Google *Spain* y Google, C-131/12, EU:C:2014:317, apartado 81.

b) Tal gestor, puede negarse a estimar una solicitud de retirada de enlaces cuando compruebe que los enlaces controvertidos dirigen a contenidos que se refieran a datos que el interesado haya hecho manifiestamente públicos y el interesado tenga derecho a oponerse a tal tratamiento por razones legítimas propias de su situación particular.

c) Dicho gestor deberá ponderar, además, si la inclusión de dicho enlace en la lista de resultados efectuada a partir del nombre del interesado es estrictamente necesaria para proteger la libertad de información de los internautas potencialmente interesados en acceder a ella, resguardando la libertad de expresión e información consagrada en el artículo 11 de la Carta.

Sobre la cuarta y quinta cuestión planteada

Otras de las cuestiones prejudiciales planteadas por el órgano jurisdiccional remitente dice relación con determinar si los datos sobre un procedimiento judicial del que es objeto una persona física y, en su caso, sobre la condena que se derive de tal procedimiento, constituyen datos relativos a las "infracciones" y a las "condenas penales", en el sentido del artículo 8, apartado 5, de la Directiva 95/46/CE, y si el gestor de un motor de búsqueda, debe acceder a la solicitud de retiro de los enlaces en la web donde figura dicha información, cuando se refieran a una etapa anterior del procedimiento judicial que no se ajuste a la situación actual.

El TJUE establece a este respecto que los datos sobre un procedimiento judicial incoado contra una persona física o su enjuiciamiento y, en su caso, la condena resultante de este, constituyen datos relativos a las "infracciones" y a las "condenas penales", en el sentido del artículo 8, apartado 5, párrafo primero, de la Directiva 95/46/CE y del artículo 10 del Reglamento 2016/679, con independencia de que durante dicho procedimiento judicial, se haya probado o no efectivamente la comisión de la infracción que se imputó a esa persona.

Por lo tanto, al incluir en la lista de resultados obtenida tras una búsqueda efectuada a partir del nombre del interesado, enlaces que dirigen a páginas webs en que se publican tales datos, el gestor de un motor de búsqueda realiza un tratamiento de estos que está sujeto a restricciones particulares donde el Derecho nacional prevea garantías apropiadas y específicas, lo que puede suceder cuando la información en cuestión, es divulgada al público por las autoridades públicas de conformidad con el Derecho nacional aplicable.

De las disposiciones contenidas tanto en la Directiva 95/46/CE[322] como del RGPD[323] se desprende que incluso un tratamiento inicialmente lícito de datos exactos puede devenir, con el tiempo, en incompatible con dicha Directiva o dicho Reglamento, cuando estos datos ya no sean necesarios en relación con los fines para los que se recogieron o trataron. Este será el caso, en particular, cuando sean inadecuados, no pertinentes o ya no pertinentes o sean excesivos en relación con estos fines considerando además el tiempo transcurrido[324].

Sin embargo, el gestor de un motor de búsqueda deberá comprobar de todos modos, considerado el interés público a que se refieren el artículo 8, apartado 4, de la Directiva[325] y el artículo 9, apartado 2, letra g), del RGPD[326], si la inclusión del enlace que dirige a la página web en cuestión, en la lista de resultados obtenida tras una búsqueda efectuada a partir del nombre del interesado, es necesaria para el ejercicio del derecho a la libertad de información de los potenciales interesados en acceder a esa página web mediante tal búsqueda, libertad de información y expresión, como ya se ha dicho, protegida por el artículo 11 de la CDFUE[327].

---

[322] Artículo 6, apartado 1, letras c) a e), que dispone: "Los Estados miembros dispondrán que los datos personales sean:… c) adecuados, pertinentes y no excesivos con relación a los fines para los que se recaben y para los que se traten posteriormente; d) exactos y, cuando sea necesario, actualizados; deberán tomarse todas las medidas razonables para que los datos inexactos o incompletos, con respecto a los fines para los que fueron recogidos o para los que fueron tratados posteriormente, sean suprimidos o rectificados; e) conservados en una forma que permita la identificación de los interesados durante un período no superior al necesario para los fines para los que fueron recogidos o para los que se traten ulteriormente. Los Estados miembros establecerán las garantías apropiadas para los datos personales archivados por un período más largo del mencionado, con fines históricos, estadísticos o científicos".

[323] Artículo 5, apartado 1, letras c) a e), que dispone: "Los datos personales serán:… c) adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados ("minimización de datos"); d) exactos y, si fuera necesario, actualizados; se adoptarán todas las medidas razonables para que se supriman o rectifiquen sin dilación los datos personales que sean inexactos con respecto a los fines para los que se tratan («exactitud»); e) mantenidos de forma que se permita la identificación de los interesados durante no más tiempo del necesario para los fines del tratamiento de los datos personales; los datos personales podrán conservarse durante períodos más largos siempre que se traten exclusivamente con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, de conformidad con el artículo 89, apartado 1, sin perjuicio de la aplicación de las medidas técnicas y organizativas apropiadas que impone el presente Reglamento a fin de proteger los derechos y libertades del interesado ("limitación del plazo de conservación")".

[324] Ver sentencia de 13 de mayo de 2014, Google *Spain* y Google, C-131/12, EU:C:2014:317, apartado 93.

[325] "Siempre que dispongan las garantías adecuadas, los Estados miembros podrán, por motivos de interés público importantes, establecer otras excepciones, además de las previstas en el apartado 2, bien mediante su legislación nacional, bien por decisión de la autoridad de control".

[326] "El tratamiento es necesario por razones de un interés público esencial, sobre la base del Derecho de la Unión o de los Estados miembros, que debe ser proporcional al objetivo perseguido, respetar en lo esencial el derecho a la protección de datos y establecer medidas adecuadas y específicas para proteger los intereses y derechos fundamentales del interesado".

[327] TEDH sentencia de 28 de junio de 2018, M.L. y W.W. c. Alemania, CE:ECHR:2018:0628JUD006079810, §§ 89 y 100 a 102, de la cual se desprende que las solicitudes dirigidas por los interesados para que se prohíba, en virtud del artículo 8 del Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales, celebrado en Roma el 4 de noviembre de 1950, que los diferentes medios de comunicación pongan en línea en Internet antiguos reportajes sobre procesos penales entablados contra esos interesados requieren que se establezca el justo equilibrio entre el derecho al respeto de la vida privada de los interesados y, en particular, la libertad de información del público. Para buscar tal equilibrio, debe tenerse en cuenta el papel esencial que la prensa desempeña en una sociedad democrática, que incluye la redacción de informes y

El TJUE dispone que corresponde al gestor de un motor de búsqueda apreciar, en el marco de una solicitud de retirada de enlaces que dirigen a páginas web en las que se publica información sobre un procedimiento judicial en materia penal incoado contra el interesado y que hace referencia a una etapa anterior de ese procedimiento que ya no corresponde a la situación actual, si a la luz del conjunto de circunstancias del caso concreto, como en particular la naturaleza y la gravedad de la infracción en cuestión, el desarrollo y el desenlace de dicho procedimiento, el tiempo transcurrido, el papel desempeñado por el interesado en la vida pública y su comportamiento en el pasado, el interés del público en el momento de la solicitud, el contenido y la forma de la publicación y las repercusiones de esta en el interesado, este tiene derecho a que la información en cuestión ya no esté, en la situación actual, vinculada a su nombre por una lista de resultados obtenida tras una búsqueda efectuada a partir de su nombre.

Como contrapartida, cuando el gestor de un motor de búsqueda constate que la inclusión del enlace controvertido es estrictamente necesaria para conciliar los derechos al respeto de la vida privada y a la protección de los datos del interesado con la libertad de información de las personas potencialmente interesadas, este gestor estará obligado, en todo caso, y a más tardar en el momento de la solicitud de retirada de enlaces, a estructurar la lista de resultados de tal manera que la imagen global que resulte de ella para el internauta refleje la situación judicial actual, lo que requerirá, en particular, que en dicha lista se indiquen en primer lugar enlaces a páginas web que contengan información al respecto.

Por todo lo expuesto el Tribunal concluye que los datos sobre un procedimiento judicial del que es objeto una persona física y, en su caso, sobre la condena que se derive de tal procedimiento sí constituyen datos relativos a las "infracciones" y a las "condenas penales", a las que se refiere el artículo 8, apartado 5, de la Directiva 95/46/CE y que el gestor de un motor de búsqueda está obligado a estimar una solicitud de retirada de enlaces que dirigen a páginas web en las que figuran tales datos, cuando estos se refieran a una etapa anterior del procedimiento judicial que no se ajusten a la situación actual, en la medida en que se constate, en el marco de la comprobación de los motivos de interés público importantes a los que se refiere el artículo 8, apartado 4, de dicha Directiva que, a la luz del conjunto de circunstancias del caso concreto, los derechos fundamentales del interesado, garantizados por los artículos 7 y 8 de la Carta, prevalecen sobre los de los internautas potencialmente interesados, protegidos por el artículo 11 de la Carta.

Sentencia C-345/17 - Buivids, de 14 de febrero de 2019

La otra sentencia por analizar es la singularizada como C-345/17 - Buivids, sentencia del Tribunal de Justicia (Sala Segunda) de 14 de febrero de 2019, cuyos hechos son los siguientes:

El Señor Sergejs Buivids grabó en video su propia declaración durante la tramitación de un expediente administrativo sancionador en los locales de una comisaría de la Policía Nacional

comentarios sobre los procedimientos judiciales. Además, a la función de los medios de comunicación que consiste en divulgar tales informaciones e ideas se añade el derecho del público a recibirlas. El Tribunal Europeo de Derechos Humanos ha reconocido, en este contexto, que el público no solo tiene interés en ser informado sobre un acontecimiento de actualidad, sino también en poder investigar acontecimientos pasados, aunque el alcance del interés del público en los procedimientos penales sea variable y pueda evolucionar a lo largo del tiempo, en función, concretamente, de las circunstancias de cada asunto.

de Letonia. El Sr. Buivids publicó el vídeo grabado, en el que aparecían varios policías y las actividades que realizaban en la comisaría, en el sitio de Internet www.youtube.com, plataforma que permite a los usuarios publicar, ver y compartir videos.

Producto de esta publicación, la *Datu valsts inspekcija* (Agencia Estatal de Protección de Datos de Letonia) resolvió, mediante una resolución de 30 de agosto de 2013, que el Sr. Buivids había infringido el artículo 8, apartado 1, de la Ley de Protección de Datos[328], pues no había proporcionado a los policías, en su condición de interesados, la información prevista en dicha disposición relativa a la finalidad del tratamiento de sus datos personales. El Sr. Buivids tampoco había proporcionado a la Agencia Estatal de Protección de Datos de ese país, información sobre la finalidad de la grabación del video controvertido y su publicación en un sitio de Internet que acreditase que el objetivo previsto era acorde con lo dispuesto en la Ley de Protección de Datos. Por consiguiente, la Agencia Estatal de Protección de Datos requirió al Sr. Buivids para que hiciera lo necesario con el fin de que este video se suprimiera del sitio de Internet www.youtube.com y de otros sitios y plataformas virtuales.

El Sr. Buivids interpuso ante la *Administratīvā rajona ties*a (Tribunal de Primera Instancia de lo Contencioso-Administrativo de Letonia) una demanda dirigida a que se declarara ilegal esta resolución de la Agencia Estatal de Protección de Datos y se reparara el perjuicio que estimaba haber sufrido. El Sr. Buivids alegó que, mediante la publicación del video controvertido, intentaba llamar la atención de la sociedad respecto a lo que, a su juicio, constituía una actuación ilegal de la policía. El citado tribunal desestimó esta demanda y luego, por sentencia de 11 de noviembre de 2015, el tribunal de alzada, la *Administratīvā apgabaltiesa* (Tribunal Regional de lo Contencioso-Administrativo de Letonia) desestimó el recurso interpuesto por el Sr. Buivids contra la sentencia de la *Administratīvā rajona tiesa* (Tribunal de Primera Instancia de lo Contencioso-Administrativo).

La *Administratīvā apgabaltiesa* (Tribunal Regional de lo Contencioso-Administrativo) basó su resolución en que, en el video controvertido, se podía ver la comisaría de policía y a varios policías ejerciendo sus funciones, así como escuchar la conversación grabada con los policías durante los trámites administrativos y las voces de policías, del Sr. Buivids y de su acompañante. Dicho tribunal consideró también, que no era posible determinar si debía primar el derecho del Sr. Buivids a la libertad de expresión o el derecho a la intimidad de otras personas, pues el Sr. Buivids no había indicado la finalidad de la publicación del vídeo controvertido.

Asimismo, en el video no se mostraban noticias de actualidad que presentasen interés para la sociedad ni una actuación deshonesta de los policías. El referido tribunal estimó que, puesto que el Sr. Buivids no había realizado su grabación con fines periodísticos con arreglo a la Ley

[328] La *Fizisko personu datu aizsardzības likums* (Ley de Protección de Datos Personales), de 23 de marzo de 2000 (*Latvijas Vēstnesis* 2000, Nº 123/124; en lo sucesivo, establece en su artículo 8, apartado 1, que: "al recoger datos personales, el responsable del tratamiento está obligado a facilitar al interesado la siguiente información, a menos que este disponga ya de ella: - La denominación, o nombre y apellido, así como la dirección, del responsable del tratamiento; - la finalidad prevista del tratamiento de los datos personales".

de Prensa y otros Medios de Información de Masas, ni con fines de expresión artística o literaria, el artículo 5 de la Ley de protección de datos no era aplicable[329].

La *Administratīvā apgabaltiesa* (Tribunal Regional de lo Contencioso-Administrativo) concluyó que, al grabar a los policías mientras desempeñaban sus funciones sin informarlos de la finalidad que tenía el tratamiento de sus datos personales, el Sr. Buivids había infringido el artículo 8, apartado 1, de la Ley de Protección de Datos.

El Sr. Buivids presentó un recurso de casación contra la sentencia de la *Administratīvā apgabaltiesa* (Tribunal Regional de lo Contencioso-Administrativo) ante el órgano jurisdiccional remitente, la *Augstākā tiesa* (Tribunal Supremo de Letonia), invocando su derecho a la libertad de expresión, argumentando que el video controvertido mostraba a funcionarios de la Policía Nacional, es decir, personas públicas, en un lugar accesible al público, que no están comprendidas, como tales, en el ámbito de aplicación de la Ley de Protección de Datos Personales.

El tribunal remitente plantea dudas, por un lado, en cuanto a si la grabación, en una comisaría de policías ejerciendo sus funciones y la publicación del video grabado en Internet, están comprendidas en el ámbito de aplicación de la Directiva 95/46/CE. A este respecto, si bien considera que el comportamiento del Sr. Buivids no está incluido en las excepciones al ámbito de aplicación de la Directiva, tal como se recoge en el artículo 3, apartado 2 de esta, puntualiza que en el caso de autos se trata de una única grabación y que el Sr. Buivids grabó a los policías en el ejercicio de sus funciones, es decir, mientras actuaban como representantes del poder público señalando que la principal preocupación que justifica que los datos personales estén protegidos, es el riesgo relacionado con su tratamiento a gran escala. Por otro lado, el tribunal remitente también plantea dudas sobre la interpretación del concepto de "con fines exclusivamente periodísticos" que figura en el artículo 9 de la Directiva 95/46/CE, y sobre si este concepto puede abarcar hechos como los imputados al Sr. Buivids.

En estas circunstancias, la *Augstākā tiesa* (Tribunal Supremo) decidió suspender el procedimiento y plantear al Tribunal de Justicia cuestiones prejudiciales que pueden resumirse así:

1. ¿Están comprendidas en el ámbito de aplicación de la Directiva 95/46/CE actividades como las controvertidas del caso en análisis, es decir, la grabación, en una comisaría de policía, de funcionarios policiales realizando trámites procedimentales y la publicación del video en el sitio de Internet www.youtube.com?

2. ¿Debe interpretarse la Directiva 95/46/CE en el sentido de que las señaladas actividades pueden considerarse como un tratamiento de datos personales con fines periodísticos, según lo dispone el artículo 9 de la Directiva 95/46/CE?

Sobre la primera cuestión planteada

[329] Según el artículo 5 de la Ley de Datos Personales, salvo disposición legal en contrario, las disposiciones de esta ley no serán de aplicación, cuando los datos personales sean objeto de tratamiento con fines periodísticos conforme al *Par presi un citiem masu informācijas līdzekļiem likums* (Ley de Prensa y otros Medios de Información de Masas), o con fines de expresión artística o literaria.

En relación con la primera cuestión prejudicial, el tribunal remitente pregunta, en esencia, si el artículo 3 de la Directiva 95/46/CE debe interpretarse en el sentido que la grabación en video de policías en una comisaría, durante una toma de declaración, y la posterior publicación del vídeo grabado en un sitio de Internet de videos en el que los usuarios pueden enviarlos, verlos y compartirlos están comprendidas en el ámbito de aplicación de esta Directiva.

Cabe recordar que, al tenor del artículo 3, apartado 1, de dicha Directiva, esta se aplicará "al tratamiento total o parcialmente automatizado de datos personales, así como al tratamiento no automatizado de datos personales contenidos o destinados a ser incluidos en un fichero".

El concepto de "datos personales" que figura en el citado precepto engloba, en virtud de la definición recogida en el artículo 2, letra a), de la misma Directiva, "toda información sobre una persona física identificada o identificable". Se considera identificable "toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante uno o varios elementos específicos, característicos de su identidad física"[330]. En el caso en análisis, se desprende que es posible ver y oír a los policías en el video controvertido, de modo que debe considerarse que las imágenes de las personas grabadas son datos personales, en el sentido del artículo 2, letra a), de la Directiva 95/46/CE.

Sobre el concepto de "tratamiento de datos personales", como ya se ha señalado en este trabajo de investigación, el artículo 2, letra b), de la Directiva 95/46/CE lo define como "cualquier operación o conjunto de operaciones (…) aplicadas a datos personales, como la recogida, registro, organización, conservación, elaboración o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma que facilite el acceso a los mismos, cotejo o interconexión, así como su bloqueo, supresión o destrucción".

Con ese marco normativo, sobre los sistemas de videovigilancia, el TJUE ya ha declarado que una grabación de video de personas almacenada en un dispositivo de grabación continua, a saber, el disco duro de dicho sistema constituye, con arreglo a los artículos 2, letra b), y 3, apartado 1, de la Directiva 95/46/CE, un tratamiento de datos personales automatizado[331]. En este mismo sentido, de la sentencia del Tribunal se extrae que el Sr. Buivids señaló que había utilizado una cámara fotográfica digital para grabar el video controvertido. Se trata entonces, de una grabación de video en la que aparecen personas, almacenada en un dispositivo de grabación continuada, esto es, la memoria de dicha cámara. De este modo, una grabación de este tipo constituye un tratamiento de datos personales automatizado, en el sentido del artículo 3, apartado 1, de la Directiva 95/46/CE.

Considerado todo expuesto el TJUE responde sobre el ámbito de aplicación de la Directiva 95/46/CE, que su artículo 3 debe interpretarse en el sentido de que la grabación en video de policías en una comisaría, durante una toma de declaración, y su posterior publicación en un sitio de Internet de vídeos, en el que los usuarios pueden enviarlos, verlos y compartirlos están comprendidas en los tratamientos de datos de carácter personal que dicha Directiva debe regular.

---

[330] Según la jurisprudencia del Tribunal de Justicia, las imágenes de una persona grabadas por una cámara constituyen "datos personales", en el sentido del artículo 2, letra a), de la Directiva 95/46, en la medida en que permiten identificar a la persona afectada. Ver en este sentido, la sentencia de 11 de diciembre de 2014, Ryneš, C-212/13, EU:C:2014:2428, apartado 22.

[331] Ver la sentencia de 11 de diciembre de 2014, Ryneš, C-212/13, EU:C:2014:2428, apartados 23 y 25.

El TJUE ha declarado que la conducta que consiste en hacer referencia en una página web a datos personales también debe considerarse un tratamiento de esta índole, ver en este sentido las sentencias de 6 de noviembre de 2003, Lindqvist, C-101/01, EU:C:2003:596, apartado 25, y de 13 de mayo de 2014, Google *Spain* y Google, C-131/12, EU:C:2014:317, apartado 26. Además, el mismo Tribunal ha precisado, por otro lado, que difundir información en una página web implica publicar dicha página en un servidor, así como realizar las operaciones necesarias para que resulte accesible a las personas que están conectadas a Internet. Estas operaciones se efectúan, al menos en parte, de manera automatizada[332].

Sobre la segunda cuestión planteada

Mediante la segunda cuestión prejudicial, el tribunal remitente consulta al TJUE si el artículo 9 de la Directiva 95/46/CE debe interpretarse en el sentido de que hechos como los controvertidos, a saber, la grabación en video de policías en una comisaría durante una toma de declaración y la publicación del video grabado en un sitio de Internet de videos en el que los usuarios pueden enviarlos, verlos y compartirlos, constituyen un tratamiento de datos personales con fines periodísticos, en el sentido de esta disposición.

> *Artículo 9 de la Directiva 95/46/CE; "Tratamiento de datos personales y libertad de expresión. En lo referente al tratamiento de datos personales con fines exclusivamente periodísticos o de expresión artística o literaria, los Estados miembros establecerán, respecto de las disposiciones del presente capítulo, del capítulo IV y del capítulo VI, exenciones y excepciones sólo en la medida en que resulten necesarias para conciliar el derecho a la intimidad con las normas que rigen la libertad de expresión".*

Sobre este punto hay que tener en cuenta el considerando 37 de la Directiva, el cual precisa que el artículo 9 de esta, tiene por objeto conciliar dos derechos fundamentales: por una parte, la protección de la intimidad y, por otra, la libertad de expresión, correspondiendo dicha compatibilidad a los Estados miembros[333].

En efecto, la Directiva dispone que, "para el tratamiento de datos personales con fines periodísticos o de expresión artística o literaria, en particular en el sector audiovisual, deben preverse excepciones o restricciones de determinadas disposiciones de la presente Directiva siempre que resulten necesarias para conciliar los derechos fundamentales de la persona con la libertad de expresión y, en particular, la libertad de recibir o comunicar informaciones, tal y como se garantiza en el artículo 10 del Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales; que por lo tanto, para ponderar estos derechos fundamentales, corresponde a los Estados miembros prever las excepciones y las restricciones necesarias en lo relativo a las medidas generales sobre la legalidad del tratamiento de datos, las medidas sobre la transferencia de datos a terceros países y las competencias de las autoridades de control sin que esto deba inducir, sin embargo, a los Estados miembros a prever excepciones a las medidas que garanticen la seguridad del tratamiento; que, igualmente, debería concederse a la autoridad de control responsable en la materia al menos una serie de

---

[332] Ver en este sentido, la sentencia de 6 de noviembre de 2003, Lindqvist, C-101/01, EU:C:2003:596, apartado 26.

[333] Ver sentencia de 16 de diciembre de 2008, *Satakunnan Markkinapörssi* y Satamedia, C-73/07, EU:C:2008:727, apartados 52 a 54.

competencias a posteriori como por ejemplo publicar periódicamente un informe al respecto o bien iniciar procedimientos legales ante las autoridades judiciales".

Incluso se desprende de la propia jurisprudencia del TJUE que las "actividades periodísticas" son las que tienen por finalidad divulgar al público información, opiniones o ideas, por cualquier medio de transmisión[334], y si bien incumbe al tribunal remitente comprobar si, en el caso en análisis, el tratamiento de datos personales que realizó el Sr. Buivids responde a esta finalidad, no es menos cierto, dice el TJUE, puede proporcionar al remitente los elementos interpretativos necesarios para que lleve a cabo el examen que le corresponde.

En efecto, el Tribunal de Justicia sostiene que el hecho de que el Sr. Buivids no sea periodista profesional, no permite excluir que la grabación del video controvertido, así como su publicación en un sitio de Internet de videos en el que los usuarios pueden enviarlos, verlos y compartirlos, pueda acogerse a lo establecido en esa disposición (artículo 9 de la Directiva), ya que el hecho de que esa grabación se haya publicado en el sitio www.youtube.com, no puede, en sí mismo, privar ese tratamiento de datos personales, de la condición de haberse efectuado "exclusivamente con fines periodísticos".

De igual forma el TJUE, advierte que no puede considerarse que cualquier información publicada en Internet, relativa a datos personales, esté comprendida dentro del concepto de "actividades periodísticas" y disfrute por ello de las exenciones y excepciones previstas en el artículo 9 de la Directiva 95/46/CE. Debiendo esto ser acreditado por el tribunal renitente.

Para ello, el tribunal remitente podrá tomar en consideración, el hecho de que, según el Sr. Buivids, el video se publicara en un sitio de Internet para llamar la atención de la sociedad sobre las prácticas supuestamente irregulares de la Policía que se desarrollaron en su toma de declaración. En cambio, si resulta que la grabación y la publicación de este video no tenían como única finalidad la divulgación al público de información, opiniones o ideas, no podrá considerarse que el tratamiento de datos personales controvertido en el litigio principal se haya realizado "con fines exclusivamente periodísticos". Además, procede recordar que las exenciones y excepciones previstas en el artículo 9 de la Directiva 95/46 solo deben aplicarse en la medida en que resulten necesarias para conciliar dos derechos fundamentales, a saber, el derecho a intimidad y el derecho a la libertad de expresión, como se analizó en la sentencia del TJUE C-136/17- GC y otros (Déréférencement de données sensibles), de 24 de septiembre de 2019, GC y otros contra Commission nationale de l'informatique et des libertés (CNIL).

Por lo que el TJUE concluye, respecto de la otra cuestión prejudicial planteada, que el artículo 9 de la Directiva 95/46/CE debe interpretarse en el sentido que hechos como los del litigio principal, a saber, la grabación en video de policías en una comisaría durante una toma de declaración y la publicación del video grabado en un sitio de Internet de videos en el que los usuarios pueden enviarlos, verlos y compartirlos, pueden constituir un tratamiento de datos personales con fines exclusivamente periodísticos, en el sentido de dicha disposición, siempre que se deduzca de dicho video que las citada grabación y publicación tienen como única finalidad la divulgación al público de información, opiniones o ideas, lo que debe comprobar el tribunal remitente.

[334] Ver sentencia de 16 de diciembre de 2008, *Satakunnan Markkinapörssi* y Satamedia, C-73/07, EU:C:2008:727, apartado 61.

Sentencia C-507/17 - Google (Portée territoriale du déréférencement), de 24 de septiembre de 2019

A continuación, se encuentra la sentencia C-507/17 - Google (*Portée territoriale du déréférencement*), sentencia del Tribunal de Justicia (Gran Sala) de 24 de septiembre de 2019, Google LLC contra *Commission nationale de l'informatique et des libertés* (CNIL), cuyos antecedentes de hecho fueron los siguientes:

Mediante resolución de 21 de mayo de 2015, la presidenta de la CNIL requirió a Google para que eliminara de su motor de búsqueda toda la lista de resultados de una persona física considerando el nombre de esta. Google se negó a este requerimiento limitándose a suprimir solo los enlaces de los resultados obtenidos como respuesta a las búsquedas efectuadas desde los nombres de dominio, correspondientes a las extensiones de su buscador en los Estados miembros de la Unión, esto es lo que se denomina un "bloqueo geográfico"[335], lo que la CNIL consideró insuficiente.

Luego de constatar que Google no había cumplido con el requerimiento en el plazo establecido, la CNIL mediante resolución de 10 de marzo de 2016, le impuso una sanción, que se hizo pública, de cien mil euros. Frente a lo cual Google se dirigió ante el Tribunal de alzada, el *Conseil d'État* (Consejo de Estado que actúa como Tribunal Supremo de lo Contencioso-Administrativo de Francia), solicitando la anulación de esa resolución.

El *Conseil d'État* (Consejo de Estado) señala que el tratamiento de datos personales que realiza el motor de búsqueda gestionado por Google está comprendido en el ámbito de aplicación de la Ley Nº 78-17, de 6 de enero de 1978, sobre informática, ficheros y libertades[336], en adelante Ley de 6 de enero de 1978, considerando las actividades de promoción y de venta de espacios publicitarios llevadas a cabo en Francia por la filial de esta sociedad, Google *France*.

El *Conseil d'État* (Consejo de Estado) señala también que el motor de búsqueda gestionado por Google se presenta con diferentes nombres de dominio empleando extensiones geográficas, a fin de adaptar los resultados que se muestran a las particularidades lingüísticas de los diferentes Estados en los que ejerce su actividad. Así, cuando la búsqueda se efectúa desde google.com, Google redirige en principio dicha búsqueda de forma automática hacia el nombre de dominio que corresponde al Estado desde el que esta se realiza, teniendo en cuenta la identificación de la dirección IP del internauta. Sin embargo, independientemente de su localización, el internauta puede realizar sus búsquedas en los demás nombres de dominio del motor. Además, aunque los resultados pueden variar en función del nombre de dominio desde el que se efectúe la búsqueda, consta que los enlaces que se obtienen como respuesta a una búsqueda proceden de bases de datos y de un trabajo de indexación comunes.

[335] Esta medida consistía en eliminar la posibilidad de acceder desde una dirección IP (Internet Protocol) supuestamente localizada en el Estado de residencia del interesado, a los resultados controvertidos obtenidos a raíz de una búsqueda efectuada a partir de su nombre.

[336] La aplicación en el derecho francés de la Directiva 95/46/CE queda garantizada mediante la *Loi* Nº 78-17, *du 6 janvier 1978, relative à l'informatique, aux fichiers et aux libertés* (Ley Nº 78-17, de 6 de enero de 1978, sobre informática, ficheros y libertades), en su versión aplicable a los hechos del litigio principal.

El *Conseil d'État* (Consejo de Estado) estima que, teniendo en cuenta, por un lado, que desde el territorio francés puede accederse a todos los nombres de dominio del motor de búsqueda de Google y, por otro lado, que existe intercambio entre esos distintos nombres de dominio, puestas de manifiesto, en particular, por el re direccionamiento automático y la presencia de identificadores de sesión, en concreto *"cookies"*, en otras extensiones del motor de búsqueda distintas de aquella en la que se colocaron inicialmente, debe considerarse que ese motor, realiza un tratamiento de datos personales único a efectos de la aplicación de la Ley de 6 de enero de 1978.

Con lo anterior, se deriva que el tratamiento de datos personales que realiza el motor de búsqueda gestionado por Google tiene lugar en una de las instalaciones de esta sociedad, Google *France*, establecida en el territorio francés, y que, por ende, está sujeto a la Ley de 6 de enero de 1978.

Ante el *Conseil d'État* (Consejo de Estado), Google sostiene que la sanción controvertida parte de una interpretación errónea de las disposiciones de la Ley de 6 de enero de 1978, que hacen aplicables los artículos 12, letra b), y 14, párrafo primero, letra a), de la Directiva 95/46/CE, sobre la base de los cuales el Tribunal de Justicia reconoció, en su sentencia de 13 de mayo de 2014, Google *Spain* y Google (C-131/12, EU:C:2014:317), un "derecho a la retirada de enlaces" de una lista de resultados. Google argumenta que ese derecho no implica necesariamente que los enlaces controvertidos deban suprimirse, sin limitación geográfica, de todos los nombres de dominio de su motor. Además, considera que, al adoptar esa interpretación, la CNIL vulneró los principios de cortesía y de no injerencia que reconoce el derecho internacional público y afectó desproporcionadamente las libertades de expresión, de información, de comunicación y de prensa, garantizadas, en particular, por el artículo 11 de la CDFUE.

Por todo lo expuesto el *Conseil d'État* (Consejo de Estado) decidió suspender el procedimiento y plantear al TJUE las siguientes cuestiones prejudiciales:

> *1. ¿Debe interpretarse el "derecho a la retirada de enlaces", según ha sido consagrado por el Tribunal de Justicia en su sentencia de 13 de mayo de 2014, Google Spain y Google (C-131/12, EU:C:2014:317), sobre la base de las disposiciones de los artículos 12, letra b), y 14, párrafo primero, letra a), de la Directiva 95/46/CE, en el sentido que el gestor de un motor de búsqueda que estima una solicitud de retirada de enlaces está obligado a proceder a dicha retirada respecto de la totalidad de los nombres de dominio de su motor, de tal manera que los [enlaces] controvertidos dejen de mostrarse independientemente del lugar desde el que se efectúe la búsqueda a partir del nombre del solicitante, incluso fuera del ámbito de aplicación territorial de la Directiva [95/46]?; 2. En caso de respuesta negativa a esta primera cuestión, ¿debe interpretarse el "derecho a la retirada de enlaces", según ha sido consagrado por el Tribunal de Justicia en su sentencia antes citada, en el sentido que el gestor de un motor de búsqueda que estima una solicitud de retirada de enlaces solamente está obligado a suprimir los enlaces controvertidos de los resultados obtenidos tras una búsqueda realizada a partir del nombre del solicitante en el nombre de dominio correspondiente al Estado en el que se considera que se ha presentado la solicitud o, de manera más general, en los nombres de dominio del motor de búsqueda que corresponden a las extensiones nacionales de dicho motor para el conjunto de los Estados miembros?; 3. Además, como complemento de la obligación mencionada en*

> *la segunda cuestión, ¿debe interpretarse el "derecho a la retirada de enlaces", según ha sido consagrado por el Tribunal de Justicia en su sentencia antes citada, en el sentido que el gestor de un motor de búsqueda que estima una solicitud de retirada de enlaces está obligado a suprimir, mediante la técnica denominada "bloqueo geográfico", desde una dirección IP supuestamente localizada en el Estado de residencia del beneficiario del "derecho a la retirada de enlaces", los resultados controvertidos obtenidos tras una búsqueda realizada a partir de su nombre, o incluso, de manera más general, desde una dirección IP supuestamente localizada en uno de los Estados miembros sujetos a la Directiva 95/46/CE, y ello independientemente del nombre de dominio utilizado por el internauta que efectúa la búsqueda?"*

Estas cuestiones prejudiciales se resumen de la siguiente manera:

1. Cuál es el alcance del "derecho a la retirada de enlaces", en el sentido de si el gestor de un motor de búsqueda, cuando acoge esa solicitud, debe retirar todos los nombres de dominio, independientemente del lugar donde se efectúa la búsqueda, incluso fuera del ámbito de aplicación de la Directiva 95/46/CE.

2. Para hacer efectivo el "derecho a la retirada de enlaces", el suprimir mediante la técnica denominada "bloqueo geográfico" afecta solo al Estado del beneficiario de tal derecho o a cualquiera de los Estados miembros afectos a la Directiva 95/46/CE, incluso a Estados que están fuera del ámbito de aplicación de tal Directiva.

Al igual que en otros fallos analizados, para abordar estas controversias el TJUE tuvo en consideración tanto las disposiciones de la Directiva 95/46/CE, vigente a la fecha de las presentaciones, como el RGPD 679/2016, que la derogó a partir del 25 de mayo del año 2018.

El TJUE delimita las cuestiones prejudiciales planteadas, determinando que procede examinarlas conjuntamente, ya que lo que se persigue resolver es si los artículos 12, letra b), y 14, párrafo primero, letra a), de la Directiva 95/46/CE y el artículo 17, apartado 1, del Reglamento 2016/679 deben interpretarse en el sentido que, cuando el gestor de un motor de búsqueda estima una solicitud de retirada de enlaces, está obligado a proceder a dicha retirada en todas las versiones de su motor de búsqueda o, por el contrario, solo está obligado a proceder a ella en las versiones de este que corresponden al conjunto de los Estados miembros, o incluso únicamente en la correspondiente al Estado miembro en el que se haya presentado la solicitud de retirada de enlaces, combinándola, en su caso, con el uso de la técnica denominada "bloqueo geográfico", a fin de garantizar que un internauta no pueda acceder, sea cual sea la versión nacional del motor de búsqueda utilizada, a los enlaces objeto del derecho de retirada, durante una búsqueda efectuada desde una dirección IP supuestamente localizada en el Estado miembro de residencia del beneficiario o, de manera más general, en cualquier otro Estado miembro.

El Tribunal de Justicia, señala que ya ha declarado que los artículos 12, letra b), y 14, párrafo primero, letra a), de la Directiva 95/46/CE deben interpretarse en el sentido que, el gestor de un motor de búsqueda está obligado a eliminar de la lista de resultados obtenida tras una búsqueda con el nombre de una persona enlaces a páginas web, publicadas por terceros y que contienen información relativa a esa persona, también en el supuesto de que este nombre o esta

información no se borren previa o simultáneamente de estas páginas web, y en su caso, aunque la publicación en dichas páginas sea en sí misma lícita[337].

Sobre este punto y como se ha expuesto en líneas anteriores, es preciso tener en cuenta los derechos fundamentales que se reconocen en los artículos 7 y 8 (respeto de la vida privada y familiar y protección de datos de carácter personal, respectivamente) de la Carta, ya que estos derechos prevalecen, en principio, no solo sobre el interés económico del gestor del motor de búsqueda, sino también sobre el interés público en acceder a información en una búsqueda que trate sobre el nombre de una persona. Con la excepción de si el interesado desempeña un papel en la vida pública, caso en el cual, la injerencia en sus derechos fundamentales está justificada por el interés preponderante de dicho público en tener, a raíz de esta inclusión, acceso a la información del interesado[338].

Como ya se ha señalado en el Reglamento 2016/679, este derecho del interesado a la retirada de enlaces se basa en el artículo 17, que regula específicamente el "derecho de supresión" o "derecho al olvido". En efecto, el artículo 17, apartado 1 del Reglamento dispone que el interesado tendrá derecho a obtener sin dilación indebida del responsable del tratamiento la supresión de los datos personales que le conciernan y el responsable del tratamiento estará obligado a suprimir lo antes posible esos datos cuando concurra alguna de las circunstancias enumeradas en dicha disposición. Por su parte el apartado 3, del artículo 17 del RGPD especifica las excepciones a esto, de entre las que se encuentran el derecho a la libertad de información de los internautas.

Tanto del artículo 4, apartado 1, letra a) de la Directiva 95/46/CE, como del artículo 3, apartado 1, del Reglamento 2016/679, se desprende que la Directiva como el Reglamento permiten a los interesados hacer valer su derecho a la retirada de enlaces frente al gestor de un motor de búsqueda que posea uno o varios establecimientos en el territorio de la Unión, en el marco de cuyas actividades realice el tratamiento de datos personales relativos a esos interesados, independientemente de que el tratamiento tenga lugar en la Unión o no.

De la controversia en análisis se colige, por un lado, que el establecimiento que Google posee en el territorio francés lleva a cabo actividades comerciales y publicitarias, que están indisolublemente vinculadas al tratamiento de datos personales necesarias para el funcionamiento del motor de búsqueda y, por otro lado, que debe considerarse que este motor de búsqueda realiza un tratamiento de datos personales único, habida cuenta, en particular, de la existencia de intercambios entre sus distintas versiones nacionales. Por lo que dicho tratamiento tiene lugar en el establecimiento de Google situado en el territorio francés. Por lo tanto, tal situación queda comprendida en el ámbito de aplicación territorial de la Directiva 95/46/CE y del Reglamento 2016/679.

Mediante estas cuestiones prejudiciales, el órgano jurisdiccional remitente desea que se dilucide el alcance territorial que cabe conferir a la retirada de enlaces en una situación de esta índole.

---

[337] Ver sentencia de 13 de mayo de 2014, Google *Spain* y Google, C-131/12, EU:C:2014:317, apartado 88.

[338] Ibídem, apartado 99.

A este respecto, del considerando 10 de la Directiva 95/46/CE y de los considerandos 10, 11 y 13 del Reglamento 2016/679, se advierte que su objetivo consiste en garantizar un elevado nivel de protección de los datos personales en toda la Unión. Y como es obvio, retirar los enlaces de todas las versiones de un motor de búsqueda responde plenamente a este objetivo.

En un mundo globalizado, el acceso de los internautas, en particular de aquellos que se hallan fuera de la Unión, a un enlace que remite a información sobre una persona cuyo centro de interés está situado en la Unión puede tener, por lo tanto, efectos inmediatos y sustanciales en la propia Unión. Tales consideraciones, señala el TJUE, podrían justificar que el legislador de la Unión fuera competente para establecer la obligación de que el gestor de un motor de búsqueda, cuando estime una solicitud de retirada de enlaces formulada por tal persona, retire dichos enlaces de todas las versiones de su motor de búsqueda.

Sin embargo, muchos terceros Estados no contemplan el derecho a la retirada de enlaces o lo abordan desde una perspectiva diferente (tal como ocurre en el caso chileno, por ejemplo). Por otra parte, como se ha señalado, el derecho a la protección de los datos personales no constituye un derecho absoluto, sino que debe considerarse en relación con su función en la sociedad manteniendo el equilibrio con otros derechos fundamentales, con arreglo al principio de proporcionalidad[339]. A esto cabe añadir que el equilibrio entre los derechos al respeto de la vida privada y a la protección de los datos personales, por un lado, y la libertad de información de los internautas, por otro, puede variar significativamente en las distintas partes del mundo.

En particular, del tenor de los artículos 12, letra b), y 14, párrafo primero, letra a), de la Directiva 95/46/CE y del artículo 17 del Reglamento 2016/679 no se desprende en modo alguno que el legislador de la Unión haya optado por atribuir a los derechos consagrados en esas disposiciones un alcance que vaya más allá del territorio de los Estados miembros y que haya pretendido imponer a un gestor que, como Google, queda comprendido en el ámbito de aplicación de la Directiva o del Reglamento, la obligación de retirar enlaces también de las versiones nacionales de su motor de búsqueda que no correspondan a los Estados miembros.

De hecho, aun cuando los artículos 56 y 60 a 66 del Reglamento 2016/679 proporcionan a las autoridades de control de los Estados miembros los instrumentos y mecanismos que les permiten, en su caso, cooperar para llegar a una decisión común basada en un equilibrio entre los derechos del interesado al respeto de su vida privada y a la protección de los datos personales que le conciernan y el interés del público de los distintos Estados miembros en tener acceso a la información, es preciso señalar que el Derecho de la Unión no prevé actualmente tales instrumentos y mecanismos de cooperación en lo que se refiere al alcance de la retirada de enlaces fuera de la Unión.

De lo anterior se deriva que el gestor de un motor de búsqueda que reciba una solicitud de retirada de enlaces presentada por el interesado, en su caso a raíz de un requerimiento de una autoridad de control o judicial de un Estado miembro, no está obligado, con arreglo al Derecho de la Unión, a proceder a retirarlo en todas las versiones de su motor de búsqueda.

[339] Ver en este sentido, la sentencia de 9 de noviembre de 2010, *Volker und Markus Schecke* y *Eifert*, C-92/09 y C-93/09, EU:C:2010:662, apartado 48.

Concluyendo el TJUE que a la luz del conjunto de consideraciones anteriores, no puede exigirse al gestor de un motor de búsqueda, que proceda a la retirada de enlaces en todas las versiones de su motor.

En relación a si procede la retirada en las versiones del motor de búsqueda correspondientes a los Estados miembros o únicamente en la versión del motor correspondiente al Estado miembro de residencia del beneficiario de la retirada de enlaces, en principio, la retirada de enlaces de que se trate debe verificarse en todos los Estados miembros, como se desprende en particular del hecho que el legislador de la Unión ha decidido establecer las normas relativas a la protección de datos mediante un reglamento, de aplicación directa y general en todos los Estados miembros[340].

Sin embargo, es importante señalar que el interés del público en acceder a una información puede variar, incluso dentro de la Unión, de un Estado miembro a otro, de modo que el resultado de la ponderación que debe llevarse a cabo entre este interés, por un lado, y los derechos al respeto de la vida privada y a la protección de los datos personales del interesado, por otro, no será necesariamente el mismo en todos los Estados miembros, más aún cuando en virtud del artículo 9 de la Directiva 95/46/CE y del artículo 85 del Reglamento 2016/679, corresponde a los Estados miembros establecer, en particular para los tratamientos realizados exclusivamente con fines periodísticos o con fines de expresión artística o literaria, las exenciones y excepciones necesarias para conciliar esos derechos con por ejemplo, la libertad de información.

> *Artículo 85 del RGPD; "Tratamiento y libertad de expresión y de información. 1. Los Estados miembros conciliarán por ley el derecho a la protección de los datos personales en virtud del presente Reglamento con el derecho a la libertad de expresión y de información, incluido el tratamiento con fines periodísticos y fines de expresión académica, artística o literaria; 2. Para el tratamiento realizado con fines periodísticos o con fines de expresión académica, artística o literaria, los Estados miembros establecerán exenciones o excepciones de lo dispuesto en los capítulos II (principios), III (derechos del interesado), IV (responsable y encargado del tratamiento), V (transferencia de datos personales a terceros países u organizaciones internacionales), VI (autoridades de control independientes), VII (cooperación y coherencia) y IX (disposiciones relativas a situaciones específicas de tratamiento de datos), si son necesarias para conciliar el derecho a la protección de los datos personales con la libertad de expresión e información; 3. Cada Estado miembro notificará a la Comisión las disposiciones legislativas que adopte de conformidad con el apartado 2 y, sin dilación, cualquier modificación posterior, legislativa u otra, de las mismas".*

[340] Así se deriva del considerando 10 del Reglamento 2016/679, con el objeto de garantizar un nivel uniforme y elevado de protección en toda la Unión y eliminar los obstáculos a la circulación de datos personales dentro de la misma.

En concreto, de los artículos 56 y 60 del Reglamento 2016/679 se desprende que, para los tratamientos transfronterizos, en el sentido del artículo 4, punto 23, del mismo[341], y con reserva de lo dispuesto en el artículo 56, apartado 2, las distintas autoridades nacionales de control interesadas deben cooperar para llegar a un consenso y a una decisión única, que vincula a todas esas autoridades y cuyo cumplimiento debe garantizar el responsable del tratamiento en lo tocante a las actividades de tratamiento en el contexto de todos sus establecimientos en la Unión.

> *Artículo 56 del RGPD; "Competencia de la autoridad de control principal 1. Sin perjuicio de lo dispuesto en el artículo 55, la autoridad de control del establecimiento principal o del único establecimiento del responsable o del encargado del tratamiento será competente para actuar como autoridad de control principal para el tratamiento transfronterizo realizado por parte de dicho responsable o encargado con arreglo al procedimiento establecido en el artículo 60. 2. No obstante lo dispuesto en el apartado 1, cada autoridad de control será competente para tratar una reclamación que le sea presentada o una posible infracción del presente Reglamento, en caso de que se refiera únicamente a un establecimiento situado en su Estado miembro o únicamente afecte de manera sustancial a interesados en su Estado miembro. 3. En los casos a que se refiere el apartado 2 del presente artículo, la autoridad de control informará sin dilación al respecto a la autoridad de control principal. En el plazo de tres semanas después de haber sido informada, la autoridad de control principal decidirá si tratará o no el caso de conformidad con el procedimiento establecido en el artículo 60, teniendo presente si existe un establecimiento del responsable o encargado del tratamiento en el Estado miembro de la autoridad de control que le haya informado. 4. En caso de que la autoridad de control principal decida tratar el caso, se aplicará el procedimiento establecido en el artículo 60. La autoridad de control que haya informado a la autoridad de control principal podrá presentarle un proyecto de decisión. La autoridad de control principal tendrá en cuenta en la mayor medida posible dicho proyecto al preparar el proyecto de decisión a que se refiere el artículo 60, apartado 3. 5. En caso de que la autoridad de control principal decida no tratar el caso, la autoridad de control que le haya informado lo tratará con arreglo a los artículos 61 y 62. 6. La autoridad de control principal será el único interlocutor del responsable o del encargado en relación con el tratamiento transfronterizo realizado por dicho responsable o encargado".*

> *Artículo 60 del RGPD; "Cooperación entre la autoridad de control principal y las demás autoridades de control interesadas 1. La autoridad de control principal cooperará con las demás autoridades de control interesadas de acuerdo con el presente artículo, esforzándose por llegar a un consenso. La autoridad de control principal y las autoridades de control interesadas se intercambiarán toda información*

[341] "…tratamiento transfronterizo": "a) el tratamiento de datos personales realizado en el contexto de las actividades de establecimientos en más de un Estado miembro de un responsable o un encargado del tratamiento en la Unión, si el responsable o el encargado está establecido en más de un Estado miembro, o b) el tratamiento de datos personales realizado en el contexto de las actividades de un único establecimiento de un responsable o un encargado del tratamiento en la Unión, pero que afecta sustancialmente o es probable que afecte sustancialmente a interesados en más de un Estado miembro".

pertinente. 2. La autoridad de control principal podrá solicitar en cualquier momento a otras autoridades de control interesadas que presten asistencia mutua con arreglo al artículo 61, y podrá llevar a cabo operaciones conjuntas con arreglo al artículo 62, en particular para realizar investigaciones o supervisar la aplicación de una medida relativa a un responsable o un encargado del tratamiento establecido en otro Estado miembro. 3. La autoridad de control principal comunicará sin dilación a las demás autoridades de control interesadas la información pertinente a este respecto. Transmitirá sin dilación un proyecto de decisión a las demás autoridades de control interesadas para obtener su dictamen al respecto y tendrá debidamente en cuenta sus puntos de vista. 4. En caso de que cualquiera de las autoridades de control interesadas formule una objeción pertinente y motivada acerca del proyecto de decisión en un plazo de cuatro semanas a partir de la consulta con arreglo al apartado 3 del presente artículo, la autoridad de control principal someterá el asunto, en caso de que no siga lo indicado en la objeción pertinente y motivada o estime que dicha objeción no es pertinente o no está motivada, al mecanismo de coherencia contemplado en el artículo 63. 5. En caso de que la autoridad de control principal prevea seguir lo indicado en la objeción pertinente y motivada recibida, presentará a dictamen de las demás autoridades de control interesadas un proyecto de decisión revisado. Dicho proyecto de decisión revisado se someterá al procedimiento indicado en el apartado 4 en un plazo de dos semanas. 6. En caso de que ninguna otra autoridad de control interesada haya presentado objeciones al proyecto de decisión transmitido por la autoridad de control principal en el plazo indicado en los apartados 4 y 5, se considerará que la autoridad de control principal y las autoridades de control interesadas están de acuerdo con dicho proyecto de decisión y estarán vinculadas por este. 7. La autoridad de control principal adoptará y notificará la decisión al establecimiento principal o al establecimiento único del responsable o el encargado del tratamiento, según proceda, e informará de la decisión a las autoridades de control interesadas y al Comité, incluyendo un resumen de los hechos pertinentes y la motivación. La autoridad de control ante la que se haya presentado una reclamación informará de la decisión al reclamante. 8. No obstante lo dispuesto en el apartado 7, cuando se desestime o rechace una reclamación, la autoridad de control ante la que se haya presentado adoptará la decisión, la notificará al reclamante e informará de ello al responsable del tratamiento. 9. En caso de que la autoridad de control principal y las autoridades de control interesadas acuerden desestimar o rechazar determinadas partes de una reclamación y atender otras partes de ella, se adoptará una decisión separada para cada una de esas partes del asunto. La autoridad de control principal adoptará la decisión respecto de la parte referida a acciones en relación con el responsable del tratamiento, la notificará al establecimiento principal o al único establecimiento del responsable o del encargado en el territorio de su Estado miembro, e informará de ello al reclamante, mientras que la autoridad de control del reclamante adoptará la decisión respecto de la parte relativa a la desestimación o rechazo de dicha reclamación, la notificará a dicho reclamante e informará de ello al responsable o al encargado. 10. Tras recibir la notificación de la decisión de la autoridad de control principal con arreglo a los apartados 7 y 9, el responsable o el encargado del tratamiento adoptará las medidas necesarias para garantizar el cumplimiento de la decisión en lo tocante a las actividades de tratamiento en el contexto de todos sus

establecimientos en la Unión. El responsable o el encargado notificarán las medidas adoptadas para dar cumplimiento a dicha decisión a la autoridad de control principal, que a su vez informará a las autoridades de control interesadas. 11. En circunstancias excepcionales, cuando una autoridad de control interesada tenga motivos para considerar que es urgente intervenir para proteger los intereses de los interesados, se aplicará el procedimiento de urgencia a que se refiere el artículo 66. 12. La autoridad de control principal y las demás autoridades de control interesadas se facilitarán recíprocamente la información requerida en el marco del presente artículo por medios electrónicos, utilizando un formulario normalizado".

Por otra parte, el artículo 61, apartado 1[342], del RGPD exige, en particular, que las autoridades de control se faciliten información útil y se presten asistencia mutua a fin de aplicar el Reglamento de manera coherente en toda la Unión, y el artículo 63[343] de dicho Reglamento precisa que, a tal efecto, se ha establecido el mecanismo de coherencia contemplado en los artículos 64 y 65 del mismo.

Artículo 64 del RGPD; "Dictamen del Comité 1. El Comité emitirá un dictamen siempre que una autoridad de control competente proyecte adoptar alguna de las medidas enumeradas a continuación. A tal fin, la autoridad de control competente comunicará el proyecto de decisión al Comité, cuando la decisión: a) tenga por objeto adoptar una lista de las operaciones de tratamiento supeditadas al requisito de la evaluación de impacto relativa a la protección de datos de conformidad con el artículo 35, apartado 4; b) afecte a un asunto de conformidad con el artículo 40, apartado 7, cuyo objeto sea determinar si un proyecto de código de conducta o una modificación o ampliación de un código de conducta es conforme con el presente Reglamento; c) tenga por objeto aprobar los criterios aplicables a la acreditación de un organismo con arreglo al artículo 41, apartado 3, o un organismo de certificación conforme al artículo 43, apartado 3; d) tenga por objeto determinar las cláusulas tipo de protección de datos contempladas en el artículo 46, apartado 2, letra d), y el artículo 28, apartado 8; e) tenga por objeto autorizar las cláusulas contractuales a que se refiere el artículo 46, apartado 3, letra a); f) tenga por objeto la aprobación de normas corporativas vinculantes a tenor del artículo 47. 2. Cualquier autoridad de control, el presidente del Comité o la Comisión podrán solicitar que cualquier asunto de aplicación general o que surta efecto en más de un Estado miembro sea examinado por el Comité a efectos de dictamen, en particular cuando una autoridad de control competente incumpla las obligaciones relativas a la asistencia mutua con arreglo al artículo 61 o las operaciones conjuntas con arreglo al artículo 62. 3. En los casos a que se refieren los apartados 1 y 2, el Comité emitirá dictamen sobre el asunto que le haya sido presentado siempre que no haya emitido ya un dictamen sobre el mismo

[342] "Las autoridades de control se facilitarán información útil y se prestarán asistencia mutua a fin de aplicar el presente Reglamento de manera coherente, y tomarán medidas para asegurar una efectiva cooperación entre ellas. La asistencia mutua abarcará, en particular, las solicitudes de información y las medidas de control, como las solicitudes para llevar a cabo autorizaciones y consultas previas, inspecciones e investigaciones".

[343] "Mecanismo de coherencia A fin de contribuir a la aplicación coherente del presente Reglamento en toda la Unión, las autoridades de control cooperarán entre sí y, en su caso, con la Comisión, en el marco del mecanismo de coherencia establecido en la presente sección".

asunto. Dicho dictamen se adoptará en el plazo de ocho semanas por mayoría simple de los miembros del Comité. Dicho plazo podrá prorrogarse seis semanas más, teniendo en cuenta la complejidad del asunto. Por lo que respecta al proyecto de decisión a que se refiere el apartado 1 y distribuido a los miembros del Comité con arreglo al apartado 5, todo miembro que no haya presentado objeciones dentro de un plazo razonable indicado por el presidente se considerará conforme con el proyecto de decisión. 4. Las autoridades de control y la Comisión comunicarán sin dilación por vía electrónica al Comité, utilizando un formato normalizado, toda información útil, en particular, cuando proceda, un resumen de los hechos, el proyecto de decisión, los motivos por los que es necesaria tal medida, y las opiniones de otras autoridades de control interesadas. 5. La Presidencia del Comité informará sin dilación indebida por medios electrónicos: a) a los miembros del Comité y a la Comisión de cualquier información pertinente que le haya sido comunicada, utilizando un formato normalizado. La secretaría del Comité facilitará, de ser necesario, traducciones de la información que sea pertinente, y b) a la autoridad de control contemplada, en su caso, en los apartados 1 y 2 y a la Comisión del dictamen, y lo publicará. 6. La autoridad de control competente no adoptará su proyecto de decisión a tenor del apartado 1 en el plazo mencionado en el apartado 3. 7. La autoridad de control contemplada en el artículo 1 tendrá en cuenta en la mayor medida posible el dictamen del Comité y, en el plazo de dos semanas desde la recepción del dictamen, comunicará por medios electrónicos al presidente del Comité si va a mantener o modificar su proyecto de decisión y, si lo hubiera, el proyecto de decisión modificado, utilizando un formato normalizado. 8. Cuando la autoridad de control interesada informe al presidente del Comité, en el plazo mencionado en el apartado 7 del presente artículo, de que no prevé seguir el dictamen del Comité, en todo o en parte, alegando los motivos correspondientes, se aplicará el artículo 65, apartado 1".

Artículo 65 del RGPD; "Resolución de conflictos por el Comité 1. Con el fin de garantizar una aplicación correcta y coherente del presente Reglamento en casos concretos, el Comité adoptará una decisión vinculante en los siguientes casos: a) cuando, en un caso mencionado en el artículo 60, apartado 4, una autoridad de control interesada haya manifestado una objeción pertinente y motivada a un proyecto de decisión de la autoridad principal, o esta haya rechazado dicha objeción por no ser pertinente o no estar motivada. La decisión vinculante afectará a todos los asuntos a que se refiera la objeción pertinente y motivada, en particular si hay infracción del presente Reglamento; b) cuando haya puntos de vista enfrentados sobre cuál de las autoridades de control interesadas es competente para el establecimiento principal; c) cuando una autoridad de control competente no solicite dictamen al Comité en los casos contemplados en el artículo 64, apartado 1, o no siga el dictamen del Comité emitido en virtud del artículo 64. En tal caso, cualquier autoridad de control interesada, o la Comisión, lo pondrá en conocimiento del Comité. 2. La decisión a que se refiere el apartado 1 se adoptará en el plazo de un mes a partir de la remisión del asunto, por mayoría de dos tercios de los miembros del Comité. Este plazo podrá prorrogarse un mes más, habida cuenta de la complejidad del asunto. La decisión que menciona el apartado 1 estará motivada y será dirigida a la autoridad de control principal y a todas las autoridades de control interesadas, y será vinculante para ellas.

3. Cuando el Comité no haya podido adoptar una decisión en los plazos mencionados en el apartado 2, adoptará su decisión en un plazo de dos semanas tras la expiración del segundo mes a que se refiere el apartado 2, por mayoría simple de sus miembros. En caso de empate, decidirá el voto del presidente. 4. Las autoridades de control interesadas no adoptarán decisión alguna sobre el asunto presentado al Comité en virtud del apartado 1 durante los plazos de tiempo a que se refieren los apartados 2 y 3. 5. El presidente del Comité notificará sin dilación indebida la decisión contemplada en el apartado 1 a las autoridades de control interesadas. También informará de ello a la Comisión. La decisión se publicará en el sitio web del Comité sin demora, una vez que la autoridad de control haya notificado la decisión definitiva a que se refiere el apartado 6. 6. La autoridad de control principal o, en su caso, la autoridad de control ante la que se presentó la reclamación adoptará su decisión definitiva sobre la base de la decisión contemplada en el apartado 1 del presente artículo, sin dilación indebida y a más tardar un mes tras la notificación de la decisión del Comité. La autoridad de control principal o, en su caso, la autoridad de control ante la que se presentó la reclamación informará al Comité de la fecha de notificación de su decisión definitiva al responsable o al encargado del tratamiento y al interesado, respectivamente. La decisión definitiva de las autoridades de control interesadas será adoptada en los términos establecidos en el artículo 60, apartados 7, 8 y 9. La decisión definitiva hará referencia a la decisión contemplada en el apartado 1 del presente artículo y especificará que esta última decisión se publicará en el sitio web del Comité con arreglo al apartado 5 del presente artículo. La decisión definitiva llevará adjunta la decisión contemplada en el apartado 1 del presente artículo".

Por último, el procedimiento de urgencia del artículo 66 del Reglamento permite, en circunstancias excepcionales, cuando una autoridad de control considere que es urgente intervenir para proteger los derechos y las libertades de los interesados, adoptar inmediatamente medidas provisionales destinadas a producir efectos jurídicos en su propio territorio, con un período de validez determinado que no podrá ser superior a tres meses.

Artículo 66 del RGPD; "Procedimiento de urgencia 1. En circunstancias excepcionales, cuando una autoridad de control interesada considere que es urgente intervenir para proteger los derechos y las libertades de interesados, podrá, como excepción al mecanismo de coherencia contemplado en los artículos 63, 64 y 65, o al procedimiento mencionado en el artículo 60, adoptar inmediatamente medidas provisionales destinadas a producir efectos jurídicos en su propio territorio, con un periodo de validez determinado que no podrá ser superior a tres meses. La autoridad de control comunicará sin dilación dichas medidas, junto con los motivos de su adopción, a las demás autoridades de control interesadas, al Comité y a la Comisión. 2. Cuando una autoridad de control haya adoptado una medida de conformidad con el apartado 1, y considere que deben adoptarse urgentemente medidas definitivas, podrá solicitar con carácter urgente un dictamen o una decisión vinculante urgente del Comité, motivando dicha solicitud de dictamen o decisión. 3. Cualquier autoridad de control podrá solicitar, motivando su solicitud, y, en particular, la urgencia de la intervención, un dictamen urgente o una decisión vinculante urgente, según el caso, del Comité, cuando una autoridad de control competente no haya tomado una medida apropiada en una situación en la que sea urgente intervenir a fin de proteger los

> *derechos y las libertades de los interesados. 4. No obstante lo dispuesto en el artículo 64, apartado 3, y en el artículo 65, apartado 2, los dictámenes urgentes o decisiones vinculantes urgentes contemplados en los apartados 2 y 3 del presente artículo se adoptarán en el plazo de dos semanas por mayoría simple de los miembros del Comité"*.

El TJUE dispone, además, que corresponde al gestor del motor de búsqueda adoptar, en caso necesario, medidas eficaces para garantizar la protección efectiva de los derechos fundamentales del interesado. Esas medidas deben respetar en sí todas las exigencias legales y deben tener como efecto impedir o, al menos, dificultar a los internautas de los Estados miembros el acceso a los enlaces de que se trate mediante una búsqueda efectuada a partir del nombre del interesado, siendo de competencia del órgano jurisdiccional remitente (Consejo de Estado) comprobar si las medidas adoptadas o propuestas por Google, cumplen estos requisitos.

Es importante señalar que, si bien el Derecho de la Unión no exige que una retirada de enlaces se realice en todas las versiones del motor de búsqueda, tampoco lo prohíbe. Por lo tanto, una autoridad de control o judicial de un Estado miembro sigue siendo competente para realizar, de conformidad con los estándares nacionales de protección de los derechos fundamentales una ponderación, por un lado entre los derechos del interesado al respeto de su vida privada y a la protección de los datos personales que le conciernan, y por otro, el derecho a la libertad de información y, al término de esta ponderación, exigir, en su caso, al gestor del motor de búsqueda que proceda a retirar los enlaces de todas las versiones de dicho motor.

El TJUE concluye que, cuando el gestor de un motor de búsqueda estime una solicitud de retirada de enlaces, estará obligado a proceder a dicha retirada no en todas las versiones de su motor, sino en las versiones de este que correspondan al conjunto de los Estados miembros, combinándola, en caso necesario, con medidas que con pleno respeto de las exigencias legales, impidan de manera efectiva o, al menos, dificulten seriamente a los internautas que efectúen una búsqueda a partir del nombre del interesado desde uno de los Estados miembros, a través de la lista de resultados que se obtenga tras esa búsqueda, a los enlaces objeto de la solicitud de retirada.

Sentencia C-673/17 - Planet49, de 1 de octubre de 2019

Luego, se encuentra la sentencia C-673/17 - Planet49, sentencia del Tribunal de Justicia (Gran Sala) de 1 de octubre de 2019, *Bundesverband der Verbraucherzentralen und Verbraucherverbände - Verbraucherzentrale Bundesverband e.V.* contra Planet49 GmbH, cuyos hechos se resumen de la siguiente manera:

El 24 de septiembre de 2013, Planet49 organizó un juego con fines promocionales en el sitio de Internet www.dein-macbook.de, quienes deseaban participar en el juego debían introducir su código postal, tras lo cual accedían a una página web en la que debían introducir su nombre y dirección. Debajo de los campos reservados para facilitar la dirección figuraban dos menciones acompañadas de casillas. La primera mención, cuya casilla (en lo sucesivo será la "primera casilla") no estaba marcada por defecto, señalaba: "Presto mi consentimiento para que determinados patrocinadores y empresas colaboradoras puedan informarme por correo, teléfono, correo electrónico o SMS sobre ofertas de su respectivo ámbito de actividad. Yo

mismo puedo determinarlos aquí, en caso contrario serán elegidos por el organizador. Puedo revocar mi consentimiento en cualquier momento. Aquí puede obtener más información al respecto".

La segunda mención, cuya casilla (en lo sucesivo, "segunda casilla") estaba marcada por defecto, tenía la siguiente redacción: "Presto mi consentimiento para el uso del servicio de análisis de páginas web Remintrex. En consecuencia, el organizador del juego con fines promocionales, (Planet49), instalará cookies una vez me haya registrado en el juego, lo que le permitirá analizar mi comportamiento de navegación y uso de páginas web de socios publicitarios y enviarme publicidad específica conforme a mis intereses a través de Remintrex. Puedo cancelar las cookies en cualquier momento. Aquí puede obtener más información".

La participación en el juego solo era posible si se marcaba, al menos, la primera casilla, la cual estaba acompañada de un enlace electrónico vinculado a las palabras "patrocinadores y empresas colaboradoras" y "aquí", que conducía a una lista en la que figuraban 57 empresas, sus direcciones, el sector de actividad publicitado y el medio de comunicación utilizado para la publicidad (correo electrónico, correo ordinario o teléfono). El término subrayado "dar de baja" figuraba después del nombre de cada empresa. La lista venía precedida del siguiente aviso: "Al hacer clic en el enlace "dar de baja", decido que no puede otorgarse a la empresa colaboradora/patrocinadora en cuestión una autorización para hacer publicidad. Si no he dado de baja a ninguna empresa colaboradora/patrocinadora o no lo he hecho en cantidad suficiente, Planet49 elegirá libremente para mí, empresas colaboradoras/patrocinadoras (número máximo: 30 empresas colaboradoras/patrocinadoras)".

Al activar el enlace electrónico que figuraba en la mención que acompañaba a la segunda casilla, vinculado al término "aquí", aparecía la siguiente información: "Las cookies utilizadas con las denominaciones ceng_cache, ceng_etag, ceng_png y gcr son pequeños ficheros que su navegador almacena en su disco duro, gracias a los cuales se facilita determinada información que hace posible una publicidad más efectiva y acorde con las preferencias del usuario. Las cookies contienen un número aleatorio (ID) que se vincula al mismo tiempo a sus datos de registro. Si usted visita posteriormente una página web de un socio publicitario registrado en Remintrex, se registrará automáticamente, gracias a un informe de Remintrex vinculado a esta, que usted (es decir, el usuario con la ID almacenada) ha visitado la página, los productos por los que se ha interesado y si se ha concluido un contrato.

Posteriormente, de acuerdo con la autorización para hacer publicidad otorgada en el momento de registrarse en el juego promocional, Planet49 puede enviarle correos publicitarios relacionados con los intereses mostrados en la página web del socio publicitario. En caso de que haya revocado la autorización publicitaria, lógicamente no volverá a recibir correos publicitarios.

La información transmitida por las cookies únicamente es utilizada para publicidad en la que se presenten productos del socio publicitario. La información será recabada, almacenada y utilizada para cada socio publicitario por separado. En ningún caso se establecerán perfiles de usuario para varios socios publicitarios. Los distintos socios publicitarios no recibirán datos personales.

En caso de que rechace el uso de cookies, las puede eliminar de su navegador en cualquier momento. En la función de ayuda de su navegador encontrará información al respecto.

A través de las cookies no se pueden ejecutar programas ni transmitir virus. De la sentencia en análisis, se desprende que las *cookies* son ficheros que el proveedor de un sitio de Internet coloca en el ordenador de los usuarios de dicho sitio y a los que puede acceder nuevamente, cuando estos vuelven a visitar el sitio, con el fin de facilitar la navegación en Internet o las transacciones o de obtener información sobre el comportamiento de dichos usuarios.

Naturalmente, tiene la posibilidad de revocar ese consentimiento en cualquier momento. La revocación deberá remitirse por escrito a Planet49. Pero también bastará un correo electrónico enviado a nuestro servicio de atención al cliente [dirección de correo electrónico]".

Frente a un requerimiento que no recibió respuesta, la *Bundesverband der Verbraucherzentralen und Verbraucherverbände - Verbraucherzentrale Bundesverband eV* (Federación de Organizaciones y Asociaciones de Consumidores o Federación de Organizaciones de Consumidores de Alemania), en lo sucesivo Federación, que figura inscrita en la lista de entidades que gozan de legitimación activa según el artículo 4 de la *Gesetz über Unterlassungsklagen bei Verbraucherrechts- und anderen Verstößen* (Ley sobre Acciones de Cesación en Caso de Infracción del Derecho de Consumo o de Otras Infracciones), de 26 de noviembre de 2001, alegó que las declaraciones de consentimiento solicitadas por Planet49 mediante las casillas primera y segunda, no cumplían los requisitos exigidos por las disposiciones del artículo 307 del *Bürgerliches Gesetzbuch* (Código Civil alemán; en lo sucesivo, BGB) del artículo 7, apartado 2, punto 2, de la *Gesetz gegen den unlauteren Wettbewerb* (Ley de Defensa de la Competencia), de 3 de julio de 2004, en su versión aplicable al litigio principal, ni tampoco se cumplían los artículos 12 y siguientes de la *Telemediengesetz*, en lo sucesivo TMG (Ley relativa a determinados servicios de comunicación e información electrónicos), de 26 de febrero de 2007, en su versión aplicable a los hechos controvertidos.

La Federación presentó una demanda ante el *Landgericht Frankfurt am Main* (Tribunal Regional de lo Civil y Penal de Fráncfort del Meno, Alemania) solicitando, sustancialmente, que se exigiese a Planet49 que dejase de pedir tales declaraciones de consentimiento y que fuera condenada a pagarle la cantidad de 214 euros, más intereses desde el 15 de marzo de 2014 en adelante. El *Landgericht Frankfurt am Main* (Tribunal Regional de lo Civil y Penal de Fráncfort del Meno) estimó parcialmente dicha demanda. Por lo que Planet49 presentó recurso de apelación ante el *Oberlandesgericht Frankfurt am Main* (Tribunal Superior Regional de lo Civil y Penal de Fráncfort del Meno, Alemania) que declaró que la pretensión de la Federación para que Planet49 dejara de incluir en los contratos de juego con fines promocionales celebrados con los consumidores, la declaración de la segunda casilla (que estaba marcada por defecto), carecía de fundamento, puesto que, por un lado, el usuario tenía conocimiento de la posibilidad de quitar la marca de dicha casilla, y, por otro , la referida mención presentaba una tipografía suficientemente clara y daba información sobre el modo de funcionamiento de las *cookies*. El Tribunal de alzada consideró asimismo que no era necesario divulgar la identidad de los terceros que podían acceder a la información recabada.

Por su parte, la Federación interpuso recurso de casación ante el *Bundesgerichtshof* (Tribunal Supremo de lo Civil y Penal), el cual declara que la solución del litigio principal depende de la interpretación de las disposiciones de los artículos 5, apartado 3 y 2, letra f), de la Directiva 2002/58, del artículo 2, letra h), de la Directiva 95/46/CE, y del artículo 6, apartado 1, letra a), del Reglamento 2016/679. Por lo que decidió suspender el procedimiento y plantear al TJUE en lo sustancial las siguientes cuestiones prejudiciales:

1. ¿Existe un consentimiento válido en el sentido de los artículos 5, apartado 3, y 2, letra f), de la Directiva 2002/58, en relación con el artículo 2, letra h), de la Directiva 95/46/CE y el artículo 6, apartado 1, letra a), del Reglamento 2016/679, cuando el almacenamiento de información o la obtención de acceso a la información ya almacenada en el equipo terminal de un usuario se autoriza a través de una casilla ya marcada, de la que el usuario debe retirar la marca en caso de que no desee prestar su consentimiento?

2. ¿Qué información debe facilitar el proveedor de servicios al usuario para cumplir con la obligación de facilitar una información clara y completa establecida en el artículo 5, apartado 3, de la Directiva 2002/58? ¿Incluye esta información también el tiempo durante el cual las *cookies* estarán activas y la cuestión de si un tercero obtiene acceso a las mismas?

Al igual que en situaciones anteriores el TJUE, resuelve estas controversias, teniendo en cuenta las disposiciones contenidas en la Directiva 95/46/CE y en el RGPD que la deroga.

Sobre la primera cuestión planteada

Una de las cuestiones prejudiciales planteadas por el órgano remitente es si los artículos 2, letra f), y 5, apartado 3, de la Directiva 2002/58, en relación con el artículo 2, letra h), de la Directiva 95/46/CE y con artículo 6, apartado 1, letra a), del Reglamento 2016/679, deben interpretarse en el sentido que el consentimiento al que se hace referencia en estas disposiciones se presta de manera válida cuando el almacenamiento de información o el acceso a la información ya almacenada en el equipo terminal del usuario de un sitio de Internet a través de *cookies* se autoriza mediante una casilla marcada por defecto, de la que el usuario debe retirar la marca en caso de que no desee prestar su consentimiento.

El TJUE precisa que, según lo señalado por el remitente, las *cookies* que pueden colocarse en el equipo terminal de los usuarios que participan en el juego con fines promocionales organizado por Planet49, llevan un número que se adjudica a los datos de registro de dicho usuario, quien debe inscribir su nombre y su dirección en el formulario de participación de dicho juego, la asociación de ese número y esos datos personaliza los datos almacenados por las *cookies* cuando el usuario utiliza Internet, de modo que la recogida de tales datos mediante las *cookies* constituye un tratamiento de datos personales.

Ahora bien, según el artículo 5, apartado 3, de la Directiva 2002/58, los Estados miembros velarán por que únicamente se permita el almacenamiento de información, o la obtención de acceso a la información ya almacenada, en el equipo terminal de un usuario cuando dicho usuario haya dado su consentimiento después de que se le haya facilitado información clara y completa, en particular sobre los fines del tratamiento de los datos, con arreglo a lo dispuesto en la Directiva 95/46/CE.

Según el tenor del artículo 5, apartado 3, de la Directiva 2002/58, procede señalar que, si bien esta disposición establece expresamente que el usuario debe haber “dado su consentimiento” a la colocación de *cookies* en su equipo terminal, sin señalar el modo o forma en que debe otorgar ese consentimiento, es procedente que se manifieste de manera clara y precisa. A este respecto, del considerando 17 de la Directiva 2002/58 se desprende que el consentimiento de

un usuario podrá darse por cualquier medio apropiado que permita la manifestación libre, inequívoca y fundada de la voluntad del usuario, por ejemplo, "mediante la selección de una casilla de un sitio web en Internet".

En este contexto el artículo 2, letra f), de la Directiva 2002/58[344], que contiene la definición de "consentimiento", se remite a la concepción de "consentimiento del interesado" que dispone la Directiva 95/46/CE, en la letra h) de su artículo 2[345]. De igual forma la Directiva 2002/58 en su considerando 17 precisa que el consentimiento de un usuario debe tener el mismo significado que el consentimiento de la persona afectada por los datos, tal como se define y se especifica en la Directiva 95/46CE. Por lo que la exigencia de una "manifestación" de voluntad del interesado sugiere claramente un comportamiento activo y no pasivo. Pues bien, según el TJUE, el consentimiento dado mediante una casilla marcada por defecto no implica un comportamiento activo por parte del usuario de un sitio de Internet.

Esta interpretación queda corroborada por el artículo 7 de la Directiva 95/46/CE, que incluye una lista exhaustiva de los casos en que un tratamiento de datos personales puede considerarse lícito y en particular en su letra a) dispone que el consentimiento del interesado puede hacer que tal tratamiento se considere lícito siempre que dicho consentimiento haya sido dado "de forma inequívoca" por el interesado. Pues bien, solo un comportamiento activo por parte del interesado, con el que manifieste su consentimiento, puede cumplir este requisito.

> *Artículo 7 de la Directiva 95/46/CE; "Los Estados miembros dispondrán que el tratamiento de datos personales sólo pueda efectuarse si: a) el interesado ha dado su consentimiento de forma inequívoca, o b) es necesario para la ejecución de un contrato en el que el interesado sea parte o para la aplicación de medidas precontractuales adoptadas a petición del interesado, o c) es necesario para el cumplimiento de una obligación jurídica a la que esté sujeto el responsable del tratamiento, o d) es necesario para proteger el interés vital del interesado, o e) es necesario para el cumplimiento de una misión de interés público o inherente al ejercicio del poder público conferido al responsable del tratamiento o a un tercero a quien se comuniquen los datos, o f) es necesario para la satisfacción del interés legítimo perseguido por el responsable del tratamiento o por el tercero o terceros a los que se comuniquen los datos, siempre que no prevalezca el interés o los derechos y libertades fundamentales del interesado que requieran protección con arreglo al apartado 1 del artículo 1 de la presente Directiva"*.

A este respecto, parece prácticamente imposible determinar de manera objetiva si el usuario de un sitio de Internet ha dado efectivamente su consentimiento para el tratamiento de sus datos personales al no quitar la marca de una casilla marcada por defecto y si dicho consentimiento ha sido dado, en todo caso, de manera informada. En efecto, no puede descartarse que dicho

[344] Además, a efectos de la presente Directiva se entenderá por: f) "consentimiento" de un usuario o abonado: el consentimiento del interesado, con arreglo a la definición de la Directiva [95/46].

[345] h) "consentimiento del interesado": toda manifestación de voluntad, libre, específica e informada, mediante la que el interesado consienta el tratamiento de datos personales que le conciernan.

usuario no haya leído la información que acompaña a la casilla marcada por defecto, o que ni siquiera la haya visto, antes de proseguir con su actividad en el sitio de Internet que visita[346].

Habida cuenta de los anteriores elementos, el consentimiento al que se hace referencia en los artículos 2, letra f), y 5, apartado 3, de la Directiva 2002/58, en relación con el artículo 2, letra h), de la Directiva 95/46/CE, no se otorga de manera válida cuando el almacenamiento de información o el acceso a información ya almacenada en el equipo terminal del usuario de un sitio de Internet se autoriza mediante una casilla marcada por defecto por el proveedor del servicio de la que el usuario debe retirar la marca en caso de que no desee prestar su consentimiento.

En el caso en análisis y a diferencia de lo que señala Planet49, el hecho de que un usuario active el botón de participación en el juego con fines promocionales no basta para considerar que el usuario ha dado de manera válida su consentimiento para la colocación de *cookies*.

Así entonces, la manifestación de voluntad a que se hace referencia en el artículo 2, letra h), de la Directiva 95/46/CE debe ser, en particular específica, en el sentido de que debe tener concretamente por objeto el tratamiento de datos de que se trate y no puede deducirse de una manifestación de voluntad que tenga un objeto distinto. En otras palabras, debe ser un consentimiento inequívoco, que se manifiesta en términos explícitos y concretos.

Esta interpretación se refuerza en el actual RGPD, que en su artículo 4, punto 11, define el consentimiento del interesado como: "*toda manifestación de voluntad libre, específica, informada e inequívoca por la que el interesado acepta, ya sea mediante una declaración o una clara acción afirmativa, el tratamiento de datos personales que le conciernen*".

Es preciso señalar a este respecto que, según el considerando 32 de dicho Reglamento, la expresión del consentimiento podría incluir, en particular, marcar una casilla de un sitio web en Internet. En cambio, dicho considerando excluye expresamente que pueda haber consentimiento en caso de silencio, casillas ya marcadas o inacción. Dice el considerando 32: "*El consentimiento debe darse mediante un acto afirmativo claro que refleje una manifestación de voluntad libre, específica, informada, e inequívoca del interesado de aceptar el tratamiento de datos de carácter personal que le conciernen, como una declaración por escrito, inclusive por medios electrónicos, o una declaración verbal. Esto podría incluir marcar una casilla de un sitio web en internet, escoger parámetros técnicos para la utilización de servicios de la sociedad de la información, o cualquier otra declaración o conducta que indique claramente en este contexto que el interesado acepta la propuesta de tratamiento de sus datos personales. Por tanto, el silencio, las casillas ya marcadas o la inacción no deben constituir consentimiento. El consentimiento debe darse para todas las actividades de tratamiento realizadas con el mismo o los mismos fines. Cuando el tratamiento tenga varios fines, debe darse el consentimiento para todos ellos. Si el consentimiento del interesado se ha*

[346] En lo que respecta a la versión original del artículo 5, apartado 3, de la Directiva 2002/58, este señalaba que el usuario tenía el "derecho de negarse" a la colocación de *cookies*, después de haber recibido, con arreglo a lo dispuesto en la Directiva 95/46/CE, información clara y completa, en particular sobre los fines del tratamiento de los datos. La Directiva 2009/136 modifico esta disposición, sustituyendo la expresión señalada por "dado su consentimiento". Así pues, el consentimiento del usuario ya no puede presumirse y debe ser un comportamiento activo del mismo.

de dar a raíz de una solicitud por medios electrónicos, la solicitud ha de ser clara, concisa y no perturbar innecesariamente el uso del servicio para el que se presta".

Teniendo en cuenta las anteriores consideraciones, el TJUE concluye respecto de esta cuestión prejudicial que los artículos 2, letra f), y 5, apartado 3, de la Directiva 2002/58, en relación con el artículo 2, letra h), de la Directiva 95/46/CE y con los artículos 4, punto 11, del Reglamento 2016/679, deben interpretarse en el sentido de que el consentimiento al que se hace referencia en estas disposiciones no se presta de manera válida cuando el almacenamiento de información o el acceso a la información ya almacenada en el equipo terminal del usuario de un sitio de Internet a través de *cookies*, se autoriza mediante una casilla marcada por defecto de la que el usuario debe retirar la marca en caso de que no desee prestar su consentimiento.

Sobre la segunda cuestión planteada

La otra cuestión prejudicial que el órgano jurisdiccional remitente pregunta, es si el artículo 5, apartado 3, de la Directiva 2002/58 debe interpretarse en el sentido de que la información que el proveedor de servicios debe facilitar al usuario de un sitio de Internet incluye el tiempo durante el cual las *cookies* estarán activas y la posibilidad de que terceros tengan acceso a ellas.

Como ya se ha señalado, el artículo 5, apartado 3, de la Directiva 2002/58 requiere que el usuario haya dado su consentimiento después de que se le haya facilitado información clara y completa, en particular sobre los fines del tratamiento de los datos. Esa información clara y completa debe permitir al usuario determinar fácilmente las consecuencias de cualquier consentimiento que pueda dar y garantizar, que dicho consentimiento se otorgue con pleno conocimiento de causa. Esa información, además, debe ser claramente comprensible y suficientemente detallada para que el usuario pueda comprender el funcionamiento de las *cookies* empleadas.

Según la controversia en análisis, las *cookies* tienen como finalidad recabar información con fines publicitarios para los productos de las empresas colaboradoras del organizador del juego promocional, la información acerca del tiempo durante el cual las *cookies* estarán activas y la posibilidad de que terceros tengan acceso a ellas forma parte de la información clara y completa, que como se señaló, debe facilitarse al usuario de conformidad con el artículo 5, apartado 3, de la Directiva 2002/58.

El artículo 10 de la Directiva 95/46/CE, enumera las indicaciones que el responsable del tratamiento debe facilitar a la persona cuyos datos recaba, estas indicaciones incluyen, en particular, además de la identidad del responsable del tratamiento y de los fines del tratamiento de que van a ser objeto los datos, cualquier otra información, como los destinatarios o las categorías de destinatarios de los datos. Si bien el tiempo durante el cual se va a proceder al tratamiento de los datos no se halla entre dichas indicaciones, de la expresión "por lo menos" se interpreta que la incluye.

> *Artículo 10 de la Directiva 95/46/CE; "Información en caso de obtención de datos recabados del propio interesado. Los Estados miembros dispondrán que el responsable del tratamiento o su representante deberán comunicar a la persona de quien se recaben los datos que le conciernan, por lo menos la información que se enumera a continuación, salvo si la persona ya hubiera sido informada de ello: a) la identidad del responsable del tratamiento y, en su caso, de su representante; b) los fines del tratamiento de que van a ser objeto los datos; c) cualquier otra información*

> *tal como: - los destinatarios o las categorías de destinatarios de los datos, - el carácter obligatorio o no de la respuesta y las consecuencias que tendría para la persona interesada una negativa a responder, - la existencia de derechos de acceso y rectificación de los datos que la conciernen, en la medida en que, habida cuenta de las circunstancias específicas en que se obtengan los datos, dicha información suplementaria resulte necesaria para garantizar un tratamiento de datos leal respecto del interesado"*.

Pues bien, el TJUE señala que debe considerarse que la información relativa al tiempo durante el cual las *cookies* estarán activas responde a la exigencia, establecida en dicho artículo, de que el tratamiento de los datos sea leal, puesto que en una situación como la controvertida, un período de tiempo largo, o incluso ilimitado, implica la recogida de numerosos datos sobre los hábitos de navegación y la frecuencia de las eventuales visitas del usuario a los sitios de los socios publicitarios del organizador del juego con fines promocionales.

Esta interpretación queda corroborada por el artículo 13, apartado 2, letra a), del Reglamento 2016/679[347], que prevé que para garantizar un tratamiento de datos leal y transparente, el responsable del tratamiento debe facilitar al interesado información, entre otras cosas, sobre el plazo durante el cual se conservarán los datos personales o, cuando no sea posible, sobre los criterios utilizados para determinar este plazo.

En lo que concierne a la posibilidad de que terceros puedan acceder o no a las *cookies*, se trata de una información comprendida en las indicaciones mencionadas en el artículo 10, letra c), de la Directiva 95/46/CE y en el artículo 13, apartado 1, letra e), del Reglamento 2016/679[348], puesto que estas disposiciones mencionan explícitamente los destinatarios o las categorías de destinatarios de los datos. Por lo que el TJUE concluye que el artículo 5, apartado 3, de la Directiva 2002/58 debe interpretarse en el sentido de que la información que el proveedor de servicios debe facilitar al usuario de un sitio de Internet incluye el tiempo durante el cual las *cookies* estarán activas y la posibilidad de que terceros tengan acceso a ellas.

Sentencia C-708/18 - Asociaţia de Proprietari bloc M5A-ScaraA, de 11 de diciembre de 2019

Finalmente, está el fallo C-708/18 - *Asociaţia de Proprietari bloc M5A-ScaraA*, Sentencia del Tribunal de Justicia (Sala Tercera) de 11 de diciembre de 2019, TK contra *Asociaţia de Proprietari bloc M5A-ScaraA* (Comunidad de Propietarios del Bloque M5A-Escalera A, Rumanía; en lo sucesivo, comunidad de propietarios), cuyos antecedentes facticos se resumen así:

[347] "Además de la información mencionada en el apartado 1, el responsable del tratamiento facilitará al interesado, en el momento en que se obtengan los datos personales, la siguiente información necesaria para garantizar un tratamiento de datos leal y transparente: a) el plazo durante el cual se conservarán los datos personales o, cuando no sea posible, los criterios utilizados para determinar este plazo".

[348] "Cuando se obtengan de un interesado datos personales relativos a él, el responsable del tratamiento, en el momento en que estos se obtengan, le facilitará toda la información indicada a continuación: e) los destinatarios o las categorías de destinatarios de los datos personales, en su caso".

TK reside en un apartamento de su propiedad situado en el edificio M5A. A petición de algunos copropietarios de ese edificio, la comunidad de propietarios aprobó, en una junta general celebrada el 7 de abril de 2016, la decisión de instalar tres cámaras de videovigilancia en las zonas comunes del edificio M5A. La primera cámara se orientó hacia la fachada del edificio, mientras que la segunda y la tercera se colocaron, respectivamente, en el vestíbulo de la planta baja y en el ascensor del edificio.

TK se opuso a la instalación de este sistema de videovigilancia, al considerar que violaba el derecho al respeto de la vida privada y pese a sus numerosas insistencias en contra de este y al reconocimiento de la ilegalidad del mismo por parte de la comunidad de propietarios, TK presentó ante el *Tribunalul Bucureşti* (Tribunal de Distrito de Bucarest, Rumanía), el órgano jurisdiccional remitente, una demanda para que obligara a la comunidad a retirar las tres cámaras y a desactivarlas definitivamente, so pena de multa.

TK alegó que el sistema de videovigilancia en cuestión infringía el Derecho originario y derivado de la Unión y el Derecho nacional, en particular lo relativo al derecho al respeto de la vida privada. Añadió que la comunidad de propietarios había asumido la función de responsable del tratamiento de los datos personales obviando el procedimiento de registro legalmente previsto a tal efecto.

La comunidad de propietarios indicó que la decisión de instalar un sistema de videovigilancia se había adoptado para controlar de la manera más efectiva posible las entradas y salidas del edificio, ya que el ascensor había sido vandalizado en varias ocasiones y varios apartamentos y zonas comunes habían sido objeto de allanamientos y robos.

La comunidad de propietarios también remitió a TK dos actas, la primera levantada en presencia de la empresa que había instalado las cámaras del sistema de videovigilancia, que indicaba que el 21 de octubre de 2016 se había procedido al borrado y a la desconexión del disco duro del sistema, que este último se había desactivado y que las imágenes grabadas habían sido eliminadas. La otra acta de 18 de mayo de 2017 daba cuenta que las tres cámaras habían sido desinstaladas mientras la comunidad de propietarios tramitaba el procedimiento de registro como responsable del tratamiento de datos personales. Pese a lo anterior, TK señaló ante el *Tribunalul Bucureşti* (Tribunal de Distrito de Bucarest, Rumanía), que las tres cámaras de videovigilancia seguían instaladas.

El órgano jurisdiccional remitente pone de manifiesto que el artículo 5 de la *Legea N° 677/2001 pentru protecţia persoanelor cu privire la prelucrarea datelor cu caracter personal şi libera circulaţie a acestor date*, en adelante Ley Nº 677/2001 (para la Protección de las Personas en relación con el Tratamiento de los Datos Personales y la Libre Circulación de Tales Datos)[349], de manera general dispone, que el tratamiento de datos personales, como la grabación de imágenes mediante un sistema de videovigilancia, solo puede llevarse a cabo con el consentimiento expreso e inequívoco del interesado. Sin embargo, el apartado 2 del mismo artículo establece una serie de excepciones a esta regla, entre las que figura la referente a la necesidad del tratamiento de datos para la protección de la vida, la integridad física o la salud del interesado o de otra persona amenazada.

[349] Monitorul Oficial al României, parte I, n.º 790, de 12 de diciembre de 2001), en su versión modificada por la Ley n.º 102/2005 y por el Decreto-ley con carácter de urgencia n.º 36/2007, aplicable ratione temporis al litigio principal, fue adoptada con el fin de transponer al Derecho rumano la Directiva 95/46/CE.

Artículo 5 de la Ley N° 677/2001; "(1) Todo tratamiento de datos personales, a menos que se refiera a datos pertenecientes a las categorías mencionadas en los artículos 7, apartado 1, 8 y 10, solo podrá llevarse a cabo si el interesado ha prestado expresa e inequívocamente su consentimiento para dicho tratamiento. (2) El consentimiento del interesado no se requerirá en los siguientes casos: a) cuando el tratamiento sea necesario para la ejecución de un contrato o precontrato en el que el interesado sea parte o para la adopción de medidas, a petición del interesado, antes de la celebración de un contrato o precontrato; b) cuando el tratamiento sea necesario para la protección de la vida, la integridad física o la salud del interesado o de otra persona amenazada; c) cuando el tratamiento sea necesario para el cumplimiento de una obligación legal del responsable del tratamiento; d) cuando el tratamiento sea necesario para el cumplimiento de una misión de interés público o inherente al ejercicio del poder público conferido al responsable del tratamiento o al tercero a quien se comuniquen los datos; e) cuando el tratamiento sea necesario para la satisfacción de un interés legítimo del responsable del tratamiento o del tercero a quien se comuniquen los datos, siempre que dicho interés no perjudique el interés o los derechos y libertades fundamentales del interesado; f) cuando el tratamiento se refiera a datos procedentes de documentos accesibles al público, de conformidad con la ley; g) cuando el tratamiento se realice exclusivamente con fines estadísticos, históricos o de investigación científica y los datos sigan siendo anónimos durante todo el tratamiento. (3) Lo dispuesto en el apartado 2 se entenderá sin perjuicio de las disposiciones legales que regulan la obligación de las autoridades públicas de respetar y proteger la vida personal, familiar y privada"

El órgano jurisdiccional remitente se refiere, en particular, al artículo 52, apartado 1, de la CDFUE[350], que establece el principio según el cual debe existir una relación de proporcionalidad entre el objetivo perseguido por la injerencia en los derechos y libertades de los ciudadanos y los medios utilizados. Según dicho órgano, el sistema de videovigilancia controvertido no parece haber sido utilizado de una manera o con una finalidad que no se corresponda con el objetivo declarado por la comunidad de propietarios, a saber, proteger la vida, la integridad física y la salud de los interesados, esto es, de los copropietarios del edificio en el que se instaló el sistema.

Dadas estas circunstancias, en lo sustancial el Tribunalul Bucureşti (Tribunal de Distrito de Bucarest, Rumanía) decidió suspender el procedimiento y plantear al TJUE la siguiente cuestión prejudicial: si los artículos 6, apartado 1, letra c), y 7, letra f), de la Directiva 95/46/CE, a la luz de los artículos 7 y 8 de la Carta, deben interpretarse en el sentido de que se oponen a disposiciones nacionales que permiten la instalación de un sistema de videovigilancia como el controvertido, colocado en las zonas comunes de un edificio de uso residencial con el fin de satisfacer intereses legítimos consistentes en garantizar el cuidado y la protección de las personas y de los bienes, sin el consentimiento de los interesados.

[350] "Cualquier limitación del ejercicio de los derechos y libertades reconocidos por la presente Carta deberá ser establecida por la ley y respetar el contenido esencial de dichos derechos y libertades. Dentro del respeto del principio de proporcionalidad, sólo podrán introducirse limitaciones cuando sean necesarias y respondan efectivamente a objetivos de interés general reconocidos por la Unión o a la necesidad de protección de los derechos y libertades de los demás".

Como ya se ha señalado en el análisis de anteriores fallos, un sistema de videovigilancia mediante cámaras debe calificarse de tratamiento automatizado de datos personales en el sentido de lo dispuesto por la Directiva 95/46/CE[351] cuando el dispositivo instalado permita grabar y almacenar datos personales, como imágenes con las que pueda identificarse a personas físicas. Correspondiendo, señala el TJUE, al órgano jurisdiccional remitente comprobar si el sistema controvertido presenta tales características.

Como ya se ha expuesto, el artículo 7 de la Directiva 95/46/CE prevé una lista exhaustiva y taxativa de los casos en los que un tratamiento de datos personales puede considerarse lícito. De ello se deduce que, para poder ser considerado legítimo, el tratamiento de datos personales debe estar comprendido en uno de los seis casos contemplados en el artículo 7 de la Directiva 95/46/CE.

Las cuestiones planteadas por el órgano jurisdiccional remitente se refieren, en particular, al principio de legitimación de las operaciones de tratamiento de datos contemplado en el artículo 7, letra f), de la Directiva 95/46/CE, disposición que fue traspuesta al ordenamiento jurídico rumano mediante el artículo 5, apartado 2, letra e), de la Ley Nº 677/2001[352], al que también remite el artículo 6 de la Decisión Nº 52/2012[353] de la Autoridad de Supervisión del Tratamiento de Datos en lo que atañe específicamente al tratamiento de datos personales mediante la videovigilancia.

Como y se ha expuesto[354], el artículo 7, letra f), de la Directiva 95/46/CE fija tres requisitos acumulativos para que el tratamiento de datos personales resulte lícito: primero, que el responsable del tratamiento o el tercero o terceros a quienes se comuniquen los datos persigan un interés legítimo; segundo, que el tratamiento de datos personales sea necesario para la satisfacción de ese interés legítimo; y tercero, que no prevalezcan sobre el interés legítimo perseguido los derechos y libertades fundamentales del interesado en la protección de los datos[355]. Es decir, el señalado artículo no establece como requisito, el consentimiento de la persona interesada, el cual si se exige en la letra a) del mismo artículo 7 de la señalada Directiva.

En la controversia en estudio, el objetivo que persigue el responsable del tratamiento de los datos cuando instala un sistema de videovigilancia es la protección de los bienes, de la salud y de la vida de los copropietarios del inmueble, lo puede calificarse de "interés legítimo" en el

---

[351] Artículo 3, apartado 1.

[352] "El consentimiento del interesado no se requerirá en los siguientes casos: e) cuando el tratamiento sea necesario para la satisfacción de un interés legítimo del responsable del tratamiento o del tercero a quien se comuniquen los datos, siempre que dicho interés no perjudique el interés o los derechos y libertades fundamentales del interesado…"

[353] La Decizia Autorității Naționale de Supraveghere a Prelucrării Datelor cu Caracter Personal nr. 52/2012 privind prelucrarea datelor cu caracter personal prin utilizarea mijloacelor de supraveghere video (Decisión de la Autoridad Nacional de Supervisión del Tratamiento de Datos Personales Nº 52/2012, relativa al tratamiento de los datos personales mediante videovigilancia), que en su artículo 6 disponía: "El tratamiento de datos personales mediante sistemas de videovigilancia se efectuará con el consentimiento expreso e inequívoco del interesado o en los casos establecidos en el artículo 5, apartado 2, de la Ley Nº 677/2001..."

[354] Ver Sentencia del Tribunal de Justicia (sala segunda) de 29 de julio de 2019. C-40/17, Fashion ID GmbH & Co. KG contra *Verbraucherzentrale NRW EV*.

[355] Ver sentencia de 4 de mayo de 2017, *Rīgas satiksme*, C-13/16, EU:C:2017:336, apartado 28.

sentido del artículo 7, letra f), de la Directiva 95/46/CE. Por lo tanto, el primer requisito fijado en esa disposición señala el TJUE parece concurrir.

En relación con el segundo requisito impuesto en el artículo 7, letra f), de la Directiva 95/46/CE, basado en la necesidad de recurrir al tratamiento de datos personales para satisfacer el interés legítimo perseguido, el Tribunal de Justicia ha recordado que las excepciones y restricciones al principio de protección de los datos de carácter personal deben establecerse sin sobrepasar los límites de lo estrictamente necesario. Por lo que el órgano jurisdiccional remitente debe comprobar que el interés legítimo del tratamiento de datos, perseguido por la videovigilancia es consistente con ello, en el sentido de garantizar la seguridad de los bienes y de las personas y en prevenir la comisión de delitos, objetivo que no puede alcanzarse razonablemente de manera tan eficaz por otros medios menos atentatorios respecto de los derechos y libertades fundamentales de los interesados, en particular respecto de los derechos al respeto de la vida privada y de protección de los datos personales, garantizados por los artículos 7 y 8 de la CDFUE.

Además, el requisito relativo a la necesidad del tratamiento debe examinarse en relación con el llamado principio de "minimización de los datos", consagrado en el artículo 6, apartado 1, letra c), de la Directiva 95/46/CE, conforme al cual los datos personales deben ser "adecuados, pertinentes y no excesivos con relación a los fines para los que se recaben y para los que se traten posteriormente".

De la controversia en análisis, el TJUE dispone que la exigencia de proporcionalidad parece haberse tenido en cuenta en el tratamiento de datos de que se trata. Consta, en efecto, y se desprende de los antecedentes analizados, que inicialmente se adoptaron medidas alternativas, consistentes en un sistema de seguridad instalado en la entrada del edificio y compuesto por un interfono y una tarjeta magnética, pero que resultaron insuficientes. Además, el sistema de videovigilancia en cuestión se limita a las zonas comunes de la copropiedad y a las vías de acceso a la misma.

Sin embargo, la proporcionalidad del tratamiento de los datos mediante un sistema de videovigilancia debe apreciarse teniendo en cuenta el modo concreto de instalación y de funcionamiento de dicho dispositivo, que debe limitar el impacto de este en los derechos y libertades de los interesados a la vez que garantizar la eficacia del mismo sistema[356].

Por último, en relación con el tercer requisito impuesto en el artículo 7, letra f), de la Directiva 95/46/CE, en relación con la existencia de derechos y libertades fundamentales del interesado en la protección de los datos, que prevalezcan sobre el interés legítimo perseguido por el responsable del tratamiento o por el tercero o terceros a los que se comuniquen los datos, hay que recordar, que la apreciación de este requisito requiere proceder a una ponderación de los derechos e intereses en conflicto a la luz de las circunstancias específicas del caso, en el marco de la cual deberá tenerse en cuenta la importancia de los derechos que los artículos 7 y 8 de la Carta confieren al interesado.

En este contexto, el Tribunal de Justicia ha declarado que el artículo 7, letra f), de la Directiva 95/46/CE se opone a que un Estado miembro excluya de manera categórica y generalizada la

[356] Por ejemplo, el requisito relativo a la necesidad del tratamiento implica que el responsable del tratamiento debe examinar, si basta con que la videovigilancia solo funcione de noche o fuera de las horas normales de trabajo, y bloquear o difuminar las imágenes tomadas en las zonas que no sea necesario vigilar.

posibilidad de someter a tratamiento determinadas categorías de datos personales, sin permitir una ponderación de los derechos e intereses en conflicto en cada caso concreto. Un Estado miembro no puede establecer con carácter definitivo el resultado de la ponderación de los derechos e intereses en conflicto respecto de tales categorías sin permitir un resultado diferente en atención a las circunstancias particulares de cada caso concreto[357].

Así entonces, el criterio relativo a la gravedad de la lesión de los derechos y libertades del interesado constituye un elemento esencial del ejercicio de ponderación, o de ponderación caso por caso, exigido por el artículo 7, letra f), de la Directiva 95/46/CE, debiendo considerarse la naturaleza de los datos personales en cuestión, en particular el carácter potencialmente sensible de los mismos, así como la naturaleza y el modo concreto del tratamiento de los datos de que se trata, en particular el número de personas que tienen acceso a ellos y el modo en que acceden.

De igual forma, tales elementos deben sopesarse en relación con la importancia, para todos los copropietarios del edificio, del interés legítimo perseguido en este caso por el sistema de videovigilancia de que se trata, en la medida en que pretende esencialmente garantizar la protección de la propiedad, de la salud y de la vida de dichos copropietarios.

Habida cuenta de las consideraciones anteriores, el TJUE responde a las cuestiones prejudiciales planteadas sobre los artículos 6, apartado 1, letra c), y 7, letra f), de la Directiva 95/46/CE, disposiciones que deben interpretarse, a la luz de los artículos 7 y 8 de la CDFUE, en el sentido de que no se oponen a disposiciones nacionales que autorizan la instalación de un sistema de videovigilancia como el controvertido en el litigio principal, colocado en las zonas comunes de un edificio de uso residencial sin el consentimiento de los interesados, con el fin de satisfacer intereses legítimos consistentes en garantizar el cuidado y la protección de las personas y de los bienes, si el tratamiento de datos personales mediante el sistema de videovigilancia de que se trata reúne los requisitos impuestos en dicho artículo 7, letra f), circunstancia que corresponde verificar al órgano jurisdiccional remitente.

Consideraciones finales

Con la precedente sentencia concluye la revisión de la jurisprudencia del Tribunal de Justicia de la Unión Europea, en materia de protección de datos de carácter personal, de cuyos fallos pueden extraerse las siguientes conclusiones generales:

1. Si bien deben ponderarse los derechos consagrados en la CDFUE, en especial los relativos al respeto de la vida privada y familiar (artículo 7) y la protección de datos de carácter personal (artículo 8), tanto con la Directiva 2002/58 relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas, como con la Directiva 95/46/CE y el RGPD, las autoridades públicas están habilitadas para acceder a ciertos y determinados datos de los titulares o interesados (nombre, apellido y dirección) por un lapso de tiempo determinado y circunscrito a la prevención, investigación, descubrimiento y persecución de delitos.

[357] Ver sentencia de 19 de octubre de 2016, Breyer, C-582/14, EU:C:2016:779, apartado 62.

2. El concepto de "responsable del tratamiento", al que alude tanto la Directiva 95/46/CE como el RGPD debe interpretarse en sentido amplio, incluyendo al administrador de una página web o de una red social, como a los proveedores de esta, o a una comunidad religiosa que en actividades de predicación puerta a puerta recoge datos de los interesados o a un gestor de un motor de búsqueda, o a una comunidad de copropietarios de un edificio que instalan cámaras de videovigilancia.

3. La autoridad de control en materia de protección de datos de un Estado de la Unión tiene la facultad para regular las sucursales de las empresas que realicen tratamiento de datos personales o actividades afines a ello (publicidad o promoción de ciertos productos), aun cuando la matriz de dicha empresa se encuentre ubicada fuera de un Estado miembro de la Unión.

4. De igual forma, la autoridad de control de un Estado miembro puede fiscalizar de manera autónoma e independiente de la autoridad de control local, a una entidad o empresa cuya matriz, este establecida en su mismo territorio, aun cuando el responsable del tratamiento de los datos tenga su domicilio en otro Estado miembro.

5. El concepto de "fichero de datos" al que alude la Directiva 95/46/CE hay que entenderlo en sentido amplio, siempre que los datos estén estructurados según criterios determinados que permitan, en la práctica, recuperarlos fácilmente para su utilización posterior. Para que dicho conjunto de datos esté comprendido en ese concepto no es preciso que incluya fichas, catálogos específicos u otros sistemas de búsqueda o sea automatizado o manual.

6. Tanto administradores como proveedores de sitios web o de redes sociales, o gestores de un motor de búsqueda, deben cumplir con el deber de información en materia de protección de datos personales.

7. La obligación de retirada de enlaces que traten datos personales incluye a los gestores de un motor de búsqueda, sin perjuicio de las excepciones que la normativa sobre protección de datos establezca, ya sea la Directiva 95/46/CE o el RGPD, compatibilizando esa obligación con la Carta de Derechos Fundamentales de la Unión Europea CDFUE, debiendo ponderar todos los antecedentes pertinentes del eventual conflicto entre la protección de datos de carácter personal y la protección a la vida privada y familiar por una parte y por la otra la libertad de expresión e información.

8. La grabación en video de funcionarios públicos en una institución pública y su posterior difusión en un sitio de Internet en el que los usuarios pueden enviarlos, verlos y compartirlos están comprendidas dentro del ámbito de aplicación de la Directiva 95/46/CE y consecuencialmente del RGPD, debiendo analizarse si dicho tratamiento de datos de carácter personal se realiza o no con fines periodísticos.

9. La gravedad de la lesión de los derechos y libertades del interesado constituye un elemento esencial del ejercicio de ponderación, o de ponderación caso por caso, exigido por el artículo 7, letra f), de la Directiva 95/46/CE, debiendo considerarse la naturaleza de los datos personales en cuestión, en particular el carácter potencialmente sensible de los mismos, así como la naturaleza y el modo concreto del tratamiento de los datos de que se trata, en particular el número de personas que tienen acceso a ellos y el modo en que acceden.

10. El gestor de un motor de búsqueda que acceda a una solicitud de retirada de enlaces, estará obligado a proceder a dicha retirada no en todas las versiones de su motor, sino en las versiones de este que correspondan al conjunto de los Estados miembros, combinándola, en caso necesario, con medidas que, con pleno respeto de las exigencias normativas, impidan de manera efectiva o, al menos, dificulten a los internautas que efectúen una búsqueda a partir del nombre del interesado desde uno de los Estados miembros el acceso, a través de la lista de resultados que se obtenga tras esa búsqueda, a los enlaces objeto de la solicitud de retirada.

11. La información que el proveedor de servicios debe facilitar al usuario de un sitio de Internet incluye el tiempo durante el cual las *cookies* estarán activas y la posibilidad de que terceros tengan acceso a ellas.

12. El consentimiento del interesado al que aluden tanto la Directiva 95/46/CE como el RGPD, no es válido cuando el almacenamiento de información o el acceso a la información ya almacenada en el equipo terminal del usuario de un sitio de Internet a través de las denominadas *cookies*, se autoriza mediante una casilla marcada por defecto de la que el usuario debe retirar la marca en caso de que no desee prestar su consentimiento, debiendo por consiguiente, dicho consentimiento ser especifico e inequívoco.

13. El interés legítimo, como una excepción al tratamiento de datos de carácter personal debe garantizar la seguridad de los bienes y de las personas, y prevenir la comisión de delitos, objetivo que no puede alcanzarse razonablemente de manera tan eficaz por otros medios menos atentatorios respecto de los derechos y libertades fundamentales de los interesados, consagrados en la CDFUE.

14. La gravedad de la lesión de los derechos y libertades del interesado constituye un elemento esencial del ejercicio de ponderación, o de ponderación caso por caso exigido, debiendo tener en cuenta la naturaleza de los datos personales en cuestión, en particular el carácter potencialmente sensible de los mismos, así como la naturaleza y el modo concreto del tratamiento de los datos de que se trata, en particular el número de personas que tienen acceso a ellos.

CAPÍTULO III

LA PROTECCIÓN DE DATOS EN AMERICA LATINA

Introducción

Si bien en el capítulo primero de este trabajo se esbozó el desarrollo que la protección de datos ha tenido en Colombia, Perú y México[358], ahora se abordará con mayor amplitud y profundidad considerando además los otros países latinoamericanos, distinguiendo si la protección de datos tiene un reconocimiento constitucional o solamente legal, teniendo en cuenta también la influencia que el Reglamento Europeo General de Protección de Datos (RGPD, Reglamento UE 2016/679) ha tenido sobre la normativa regional.

Antes de entrar al análisis de la normativa latinoamericana, se considerará también la regulación a nivel iberoamericano radicada en instrumentos de *soft law* fuertemente influenciados por el RGPD de la UE, así como los Principios para la Protección de Datos recientemente actualizados en abril del año 2021, por la Organización de Estados Americanos – OEA. Igualmente se revisará la regulación estadounidense en la materia, especialmente la más reciente legislación en protección de datos de ese país, circunscrita al Estado de California, la que entró en vigor el primero de enero del año 2020.

Como se sabe, si bien la protección de datos está en un intenso proceso de desarrollo, este ha sido afectado por la pandemia del COVID 19 que tan severamente ha azotado a la población mundial y, en especial a los países latinoamericanos, donde la data e información de contagiados y muertes no se ofrecen de forma estandarizada. En muchos países tampoco existe una autoridad de control que permita garantizar el derecho a la privacidad y a la protección de datos de carácter personal. A diferencia de lo que ocurre en otras latitudes, como la europea, donde varios Estados miembros han adoptado medidas de emergencia en un esfuerzo por proteger la salud pública, compatibilizándola con la protección de datos de carácter personal[359].

Cualquier restricción debe respetar el contenido esencial de los derechos y libertades fundamentales, configurándose como una medida necesaria y proporcionada en una sociedad democrática para salvaguardar un interés público como, por ejemplo, la salud pública. Dado que se están eliminando progresivamente las medidas de contención, los responsables de la toma de decisiones deben dar respuesta a las expectativas de los ciudadanos, respuestas que ofrezcan soluciones digitales fiables y respetuosas de los derechos a la intimidad y a la protección de los datos personales.

Por lo anterior, en muchos países, las medidas de protección de la privacidad incorporadas, como la inscripción voluntaria por los usuarios, la minimización y la seguridad de los datos o la exclusión de la geolocalización, se consideran esenciales para garantizar la fiabilidad y la aceptación social de las soluciones basadas en datos destinados a controlar y contener la

[358] Ver páginas 72 a 74 de esta misma obra.

[359] Véase los documentos de la Agencia Española de Protección de Datos en relación con el COVID-19 en https://www.aepd.es/es/areas-de-actuacion/proteccion-datos-y-coronavirus

propagación del virus, calibrar las contramedidas de política pública, ayudar a los pacientes o aplicar estrategias de salida a la pandemia.

En la UE, el marco normativo en materia de protección de datos y privacidad ha demostrado ser una herramienta lo suficientemente flexible para permitir el desarrollo de soluciones prácticas, como por ejemplo, las aplicaciones de rastreo, garantizando al mismo tiempo un elevado nivel de protección de los datos personales. En este contexto, el 16 de abril de 2020, la Comisión publicó unas orientaciones sobre las aplicaciones móviles de apoyo a la lucha contra la pandemia en lo referente a la protección de datos[360].

Este creciente y hasta vertiginoso desarrollo tiene sin dudarlo su fundamento en el avance que también han tenido las nuevas tecnologías, las TIC y el *Big data*, lo que según el Grupo de Trabajo del Artículo 29 del RGPD, genera diversas complejidades y riesgos significativos para la protección de los datos personales y el derecho a la privacidad. En particular, el *big data* plantea preocupaciones sobre: la escala de la recopilación de datos; el seguimiento y la elaboración de perfiles, teniendo también en cuenta la variedad y los detalles de los datos recopilados y el hecho de que los datos a menudo se combinan de muchas fuentes diferentes; la seguridad de los datos, con niveles de protección que se han demostrado van por detrás de la expansión de su volumen. Sumado a la afectación de los particulares los cuales a menos que se les proporcione información suficiente, estarán sujetos a decisiones que no entienden y sobre las cuales no tienen control, produciendo eventualmente inexactitud, discriminación, exclusión y desequilibrio económico.[361]

En el ámbito latinoamericano, como ya se ha señalado, si bien aún no existe una norma internacional de carácter vinculante sobre la protección de datos, existen dos instancias multilaterales donde se ha abordado y reconocido la necesidad de regular y tutelar el derecho a la protección de datos de carácter personal. La primera es la establecida por la Red Iberoamericana de Protección de Datos, a la que adscriben voluntariamente más de una decena de países y; la segunda, es la Organización de Estados Americanos, OEA, que por encargo de su Asamblea General, hizo que el Departamento de Derecho Internacional y el Comité Jurídico Interamericano emitieran informes y pronunciamientos sobre el tema. En las siguientes líneas se abordaran tales regulaciones.

---

[360] Comunicación de la Comisión "Orientaciones sobre las aplicaciones móviles de apoyo a la lucha contra la pandemia de COVID-19 en lo referente a la protección de datos" 2020/C 124 I/01 – C (2020) 2523 - (DO C 124I de 17.4.2020, p. 1). El 16 de abril de 2020, los Estados miembros de la UE, con el apoyo de la Comisión, desarrollaron un conjunto de instrumentos de la UE para el uso de aplicaciones móviles de rastreo de contactos y alerta en respuesta a la pandemia de coronavirus. Esto forma parte de un enfoque coordinado común para apoyar la supresión gradual de las medidas de confinamiento. Ver: https://ec.europa.eu/health/sites/health/files/ehealth/docs/covid-19_apps_en.pdf

[361] Ver página 45, https://ec.europa.eu/justice/article-29/ documentation/opinion-recommendation/files/2013/wp203_en.pdf consulta realizada el 13 de julio 2020, el texto original señala: *"Despite its potential for innovation, big data may also pose significant risks for the protection of personal data and the right to privacy. In particular, big data raises concerns about: - the sheer scale of data collection, tracking and profiling, also taking into account the variety and detail of the data collected and the fact that data are often combined from many different sources; - the security of data, with levels of protection shown to be lagging behind the expansion in volume; - transparency: unless they are provided with sufficient information, individuals will be subject to decisions that they do not understand and have no control over; - inaccuracy, discrimination, exclusion and economic imbalance (as will be discussed further below); and - increased possibilities of government surveillance"*.

Estándares para la Protección de Datos en los países Iberoamericanos de la Red Iberoamericana

La Red Iberoamericana de Protección de Datos[362] integrada por doce Estados miembros, México, Andorra, España, Argentina, Brasil, Chile, Colombia, Costa Rica, Panamá, Perú, Portugal y Uruguay, en el año 2017[363] aprobó los Estándares para la Protección de Datos en los países Iberoamericanos, documento que declara entre sus principales objetivos: "Establecer un conjunto de principios y derechos comunes de protección de datos personales que los Estados Iberoamericanos puedan adoptar y desarrollar en su legislación nacional, con la finalidad de contar con reglas homogéneas en la región; Garantizar el efectivo ejercicio y tutela del derecho a la protección de datos personales de cualquier persona física en los Estados Iberoamericanos, mediante el establecimiento de reglas comunes que aseguren el debido tratamiento de sus datos personales; Facilitar el flujo de los datos personales entre los Estados Iberoamericanos y más allá de sus fronteras, con la finalidad de coadyuvar al crecimiento económico y social de la región; Favorecer la cooperación internacional entre las autoridades de control de los Estados Iberoamericanos, con otras autoridades de control no pertenecientes a la región y autoridades y organismos internacionales en la materia".

Estas directrices, si bien no son vinculantes ni obligatorias, son expresión del esfuerzo común de los países del Bloque Iberoamericano por dotarse de una normativa común. Estos Estándares se contienen en un documento de treintaicuatro páginas, que consta de un preámbulo y veintiséis considerandos, además de diez capítulos y cuarenta y cinco artículos. El capítulo primero trata sobre "Disposiciones Generales", el capítulo segundo sobre "Principios de protección de datos personales", el capítulo tercero se refiere a los "Derechos del titular", el capítulo cuarto aborda el "Encargado", el capítulo quinto regula las "Transferencias internacionales de datos personales", el capítulo sexto trata sobre las "Medidas proactivas en el tratamiento de datos personales", el capítulo séptimo sobre la "Autoridad de Control", el capítulo octavo se refiere a las "Reclamaciones y Sanciones", el capítulo noveno sobre "Derecho a la indemnización" y el capítulo décimo aborda la "Cooperación internacional".

El artículo uno, apartado 1 de los Estándares establece cuáles son sus finalidades y objeto:

> *"Los presentes Estándares tienen por objeto:*
> *a. Establecer un conjunto de principios y derechos de protección de datos personales que los Estados Iberoamericanos puedan adoptar y desarrollar en su legislación nacional, con la finalidad de garantizar un debido tratamiento de los datos personales y contar con reglas homogéneas en la región.*

[362] Desde el año 1996 la Asamblea General (AG) de la OEA ha venido aprobando resoluciones sobre el tema de la protección de datos personales**.** El tema también ha figurado en la agenda del Comité Jurídico Interamericano (CJI) el cual en 2000 presentó un documento sobre "El Derecho de la información: acceso y protección de la información y datos personales en formato electrónico." Desde ese año, el CJI siguió trabajando en esa área, adoptando una serie de documentos. Particularmente, en 2012 el CJI aprobó una "Propuesta de Declaración de Principios de Privacidad y Protección de Datos Personales en las Américas", que contiene 12 principios sobre la materia, y en 2015, la "Guía Legislativa sobre la Privacidad y la Protección de Datos Personales en las Américas".

[363] Ver: https://www.redipd.org/sites/default/files/inline-files/Estandares_Esp_Con_logo_RIPD.pdf. Consulta realizada el 13 de julio de 2020.

b. Elevar el nivel de protección de las personas físicas en lo que respecta al tratamiento de sus datos personales, así como entre los Estados Iberoamericanos, el cual responda a las necesidades y exigencias internacionales que demanda el derecho a la protección de datos personales en una sociedad en la cual las tecnologías de la información y del conocimiento cobran cada vez mayor relevancia en todos los quehaceres de la vida cotidiana.

c. Garantizar el efectivo ejercicio y tutela del derecho a la protección de datos personales de cualquier persona física en los Estados Iberoamericanos, mediante el establecimiento de reglas comunes que aseguren el debido tratamiento de sus datos personales.

d. Facilitar el flujo de los datos personales entre los Estados Iberoamericanos y más allá de sus fronteras, con la finalidad de coadyuvar al crecimiento social y económico de la región.

e. Impulsar el desarrollo de mecanismos para la cooperación internacional entre las autoridades de control de los Estados Iberoamericanos, autoridades de control no pertenecientes a la región y autoridades y entidades internacionales en la materia".

El apartado 2 del artículo primero de estos Estándares se refiere a las definiciones;

"Para los efectos de los presentes Estándares se entenderá por:

*a. **Anonimización:** la aplicación de medidas de cualquier naturaleza dirigidas a impedir la identificación o reidentificación de una persona física sin esfuerzos desproporcionados.*

*b. **Consentimiento:** manifestación de la voluntad, libre, específica, inequívoca e informada, del titular a través de la cual acepta y autoriza el tratamiento de los datos personales que le conciernen.*

*c. **Datos Personales**: cualquier información concerniente a una persona física identificada o identificable, expresada en forma numérica, alfabética, gráfica, fotográfica, alfanumérica, acústica o de cualquier otro tipo. Se considera que una persona es identificable cuando su identidad pueda determinarse directa o indirectamente, siempre y cuando esto no requiera plazos o actividades desproporcionadas.*

*d. **Datos personales sensibles**: aquellos que se refieran a la esfera íntima de su titular, o cuya utilización indebida puedan dar origen a discriminación o conlleve un riesgo grave para éste. De manera enunciativa, se consideran sensibles los datos personales que puedan revelar aspectos como origen racial o étnico; creencias o convicciones religiosas, filosóficas y morales; afiliación sindical; opiniones políticas; datos relativos a la salud, a la vida, preferencia u orientación sexual, datos genéticos o datos biométricos dirigidos a identificar de manera unívoca a una persona física.*

*e. **Encargado**: prestador de servicios, que, con el carácter de persona física o jurídica o autoridad pública, ajena a la organización del responsable, trata datos personales a nombre y por cuenta de éste.*

*f. **Exportador**: persona física o jurídica de carácter privado, autoridad pública, servicios, organismo o prestador de servicios situado en territorio de un Estado que efectúe transferencias internacionales de datos personales, conforme a lo dispuesto en los presentes Estándares.*

g. ***Responsable****: persona física o jurídica de carácter privado, autoridad pública, servicios u organismo que, solo o en conjunto con otros, determina los fines, medios, alcance y demás cuestiones relacionadas con un tratamiento de datos personales.*
h. ***Titular****: persona física a quien le conciernen los datos personales.*
i. ***Tratamiento:*** *cualquier operación o conjunto de operaciones efectuadas mediante procedimientos físicos o automatizados realizadas sobre datos personales, relacionadas, de manera enunciativa más no limitativa, con la obtención, acceso, registro, organización, estructuración, adaptación, indexación, modificación, extracción, consulta, almacenamiento, conservación, elaboración, transferencia, difusión, posesión, aprovechamiento y en general cualquier uso o disposición de datos personales".*

Luego, su artículo tres aborda el ámbito de aplicación subjetivo de los mismos al señalar: *"Los presentes Estándares serán aplicables a las personas físicas o jurídicas de carácter privado, autoridades y organismos públicos, que traten datos personales en el ejercicio de sus actividades y funciones".* Seguidamente el artículo 4 regula su ámbito de aplicación objetivo, señalando al respecto que, "*Los presentes Estándares serán aplicables al tratamiento de datos personales que obren en soportes físicos, automatizados total o parcialmente, o en ambos soportes, con independencia de la forma o modalidad de su creación, tipo de soporte, procesamiento, almacenamiento y organización*" (artículo 4.1). Y a continuación que "*Por regla general, los presentes Estándares serán aplicables a los datos personales de personas físicas, lo cual no impide que los Estados Iberoamericanos en su legislación nacional dispongan que la información de las personas jurídicas sea salvaguardada acorde con el derecho a la protección de datos personales, en cumplimiento a lo establecido en su derecho interno*" (artículo 4.2).

Estos Estándares al igual que el RGPD, aunque de manera no vinculante, incorporan disposiciones muy relevantes para el adecuado tratamiento de datos personales en la era digital, como la aplicación extraterritorial de sus disposiciones, cuando el encargado o responsable de tratamiento no se encuentre establecido en el territorio de algún país iberoamericano, pero las actividades de tratamiento estén relacionadas con la oferta de bienes o servicios dirigidos a residentes iberoamericanos. Así se desprende de su artículo 5.1, que señala:

"Los Estándares serán aplicables al tratamiento de datos personales efectuado:

a. Por un responsable o encargado establecido en territorio de los Estados Iberoamericanos.

b. Por un responsable o encargado no establecido en territorio de los Estados Iberoamericanos, cuando las actividades del tratamiento estén relacionadas con la oferta de bienes o servicios dirigidos a los residentes de los Estados Iberoamericanos, o bien, estén relacionadas con el control de su comportamiento, en la medida en que éste tenga lugar en los Estados Iberoamericanos.

c. Por un responsable o encargado que no esté establecido en un Estado Iberoamericano, pero le resulte aplicable la legislación nacional de dicho Estado, derivado de la celebración de un contrato o en virtud del derecho internacional público. d. Por un responsable o encargado no establecido en territorio de los Estados Iberoamericanos y que utilice o recurra a medios, automatizados o no, situados en ese territorio para tratar datos personales, salvo que dichos medios se utilicen solamente con fines de tránsito".

Los Estándares Iberoamericanos también consagran en su capítulo segundo una serie de principios que recogen la experiencia principalmente europea en la materia, al establecer desde los artículos diez al veintitrés los Principios de protección de datos personales.

Del mismo modo, entre los artículos veinticuatro al veintiocho se establecen los denominados derechos ARCO; de acceso (artículo 25)[364], rectificación (artículo 26)[365], cancelación (artículo 27)[366] y oposición (artículo 28)[367]. También los Estándares garantizan el derecho de las personas físicas a no ser objeto de decisiones automatizadas que produzcan efectos jurídicos o similares cuando no medie intervención humana.

> *"Artículo 29. Derecho a no ser objeto de decisiones individuales automatizadas*
> *.1. El titular tendrá derecho a no ser objeto de decisiones que le produzcan efectos jurídicos o le afecten de manera significativa que se basen únicamente en tratamientos automatizados destinados a evaluar, sin intervención humana, determinados aspectos personales del mismo o analizar o predecir, en particular, su rendimiento profesional, situación económica, estado de salud, preferencias sexuales, fiabilidad o comportamiento.*
> *.2. Lo dispuesto en el numeral anterior no resultará aplicable cuando el tratamiento automatizado de datos personales sea necesario para la celebración o la ejecución de un contrato entre el titular y el responsable; esté autorizado por el derecho interno de los Estados Iberoamericanos, o bien, se base en el consentimiento demostrable del titular.*
> *3. No obstante, cuando sea necesario para la relación contractual o el titular hubiere manifestado su consentimiento tendrá derecho a obtener la intervención humana; recibir una explicación sobre la decisión tomada; expresar su punto de vista e impugnar la decisión. 29*
> *4. El responsable no podrá llevar a cabo tratamientos automatizados de datos personales que tengan como efecto la discriminación de los titulares por su origen racial o étnico; creencias o convicciones religiosas, filosóficas y morales; afiliación sindical; opiniones políticas; datos relativos a la salud, a la vida, preferencia u orientación sexual, así como datos genéticos o datos biométricos".*

De igual manera estos Estándares abordan en los diferentes apartados del artículo cuarenta y dos, la regulación de la autoridad de control y los requisitos para su instalación, así como sus características y facultades para ejercer sus funciones y poderes.

> *Artículo 42. "Naturaleza de las autoridades de control y supervisión*

---

[364] "El titular tendrá el derecho de solicitar el acceso a sus datos personales que obren en posesión del responsable, así como a conocer cualquier información relacionada con las condiciones generales y específicas de su tratamiento".

[365] "El titular tendrá el derecho a obtener del responsable la rectificación o corrección de sus datos personales, cuando éstos resulten ser inexactos, incompletos o no se encuentren actualizados".

[366] "El titular tendrá derecho a solicitar la cancelación o supresión de sus datos personales de los archivos, registros, expedientes y sistemas del responsable, a fin de que los mismos ya no estén en su posesión y dejen de ser tratados por este último".

[367] "El titular podrá oponerse al tratamiento de sus datos personales cuando: a. Tenga una razón legítima derivada de su situación particular. b. El tratamiento de sus datos personales tenga por objeto la mercadotecnia directa, incluida la elaboración de perfiles, en la medida que esté relacionada con dicha actividad".

1. *En cada Estado Iberoamericano deberá existir una o más autoridades de control en materia de protección de datos personales con plena autonomía, de conformidad con su legislación nacional aplicable en la materia.*
2 *Las autoridades de control podrán ser órganos unipersonales o pluripersonales; actuarán con carácter imparcial e independiente en sus potestades, así como serán ajenas a toda influencia externa, ya sea directa o indirecta, y no solicitarán ni admitirán orden ni instrucción alguna.*
3. *El miembro o los miembros de los órganos de dirección de las autoridades de control deberán contar con la experiencia y aptitudes, en particular respecto al ámbito de protección de datos personales, necesarios para el cumplimiento de sus funciones y el ejercicio de sus potestades. Se nombrarán mediante un procedimiento transparente en virtud de la legislación nacional aplicable y únicamente podrán ser removidos por causales graves establecidas en el derecho interno de cada Estado Iberoamericano, conforme a las reglas del debido proceso.*
4. *La legislación nacional de los Estados Iberoamericanos que resulte aplicable en la materia deberá otorgar a las autoridades de control suficientes poderes de investigación, supervisión, resolución, promoción, sanción y otros que resulten necesarios para garantizar el efectivo cumplimiento de ésta, así como el ejercicio y respeto efectivo del derecho a la protección de datos personales.*
5. *Las decisiones de las autoridades de control únicamente estarán sujetas al control jurisdiccional, conforme a los mecanismos establecidos en la legislación nacional de los Estados Iberoamericanos que resulte aplicable en la materia y su derecho interno.*
6. *Las autoridades de control deberán contar con los recursos humanos y materiales necesarios para el cumplimiento de sus funciones".*

Los señalados Estándares de Protección de datos, han sido ratificados y complementados con el documento "La Red Iberoamericana de Protección de Datos (RIPD) 2020" "(Documento estratégico sobre el futuro de la RIPD)"[368], que entre sus objetivos busca actualizar las directrices para "que sirvan de parámetro para futuras regulaciones o para la revisión de las existentes. Asimismo, se entiende pertinente la elaboración y difusión de guías y recomendaciones en áreas prioritarias y de vanguardia tecnológica, la elaboración y difusión de documentos de referencia normativos y el desarrollo de una base de datos de jurisprudencia en Protección de Datos PDP". Esta actualización que la instancia Iberoamericana persigue da cuenta como se ha señalado, del vertiginoso cambio que de manera continua representa el *big data*, las TIC y el internet de las cosas.

También el señalado documento expresa la globalidad y transversalidad que la regulación y tutela de la protección de datos representa, promoviendo que la Red interactúe y establezca vínculos más estrechos con instancias multilaterales abocadas a la protección de datos como la Relatoría Especial de NU sobre el Derecho a la Privacidad, o promover acuerdos con las autoridades de protección de datos de la Unión Europea y con otras Redes, en especial con la Red Francófona de Protección de Datos Personales (AFAPDP). Del mismo modo se plantea el desarrollo de un dialogo "con otras partes interesadas (*stakeholders*) fuera de la región". En

[368] Ver:https://www.redipd.org/sites/default/files/inline-files/Texto_definitivo_RIPD_2020.pdf. Consulta realizada el 13 de julio de 2020.

este sentido como ejemplo cabe tener en cuenta el proyecto *Privacy Bridges* impulsado por el entonces titular de la Autoridad Holandesa.

Concluye el documento, señalando que estas definiciones estratégicas deben ser plasmadas en un nuevo Reglamento de la Red Iberoamericana de Protección de Datos[369], tal como se señala en su apartado "III. Cambios Reglamentarios", lo que "va a exigir una adaptación a fondo del Reglamento de la RIPD, que no sería más que una continuación del camino iniciado en el XI Encuentro de Cartagena de Indias con el llamado "proceso de institucionalización" de la RIPD".

Principios de la Protección de Datos de la Organización de Estados Americanos (OEA)

El 9 de abril del año 2021 el Comité Jurídico Interamericano (CJI) aprobó los Principios Actualizados sobre privacidad y protección de datos personales[370]. Resultado del trabajo que se inició el año 2018 por mandato de la Asamblea General de la OEA, con la finalidad de generar un documento que diera cuenta del desarrollo de la temática en la región, así como contribuir al establecimiento de ciertos estándares comunes en materia de privacidad y protección de datos.

Se señala en la Resolución 266 (XCVIII/21) del Comité Jurídico Interamericano (CJI), que este procedió a la actualización de los "Principios sobre Privacidad y Protección de Datos Personales, con Anotaciones" adoptados en el año 2015 por el CJI como guía legislativa para los Estados miembros de la OEA, dicha actualización se produce en el contexto de los desarrollos normativos internacionales ocurridos desde el 2015 a la fecha. Realizando una revisión exhaustiva y minuciosa de los Principios, anotados a la luz de los avances más recientes a nivel internacional, la relatoría del tema llevó a cabo un proceso de consultas entre agosto de 2020 y febrero de 2021, abierto a todos los Estados miembros y algunas entidades internacionales con el fin de incorporar estos valiosos insumos en su revisión, para producir un documento que refleje las distintas aproximaciones que sobre el tema coexisten en la región, resolviendo aprobar los "Principios Actualizados sobre la Privacidad y la Protección de los Datos Personales, con Anotaciones"[371], los cuales se encuentran contenidos en el respectivo anexo de esa Resolución.

La actualización de estos principios da cuenta de la relevancia de promover y armonizar entre los países de la región las cuestiones relativas a dichas materias, estableciendo directrices relacionadas con la transparencia en el tratamiento de los datos, la rendición de cuentas, la seguridad de los datos sensibles, la agilización del comercio nacional e internacional y el empoderamiento de la ciudadanía respecto del tratamiento de sus datos personales.

---

[369] El Reglamento vigente de la RIPD puede consultarse en: https://www.redipd.org/sites/default/files/inline-files/REGLAMENTO_RIPD_DIC2018.pdf

[370] Ver en: CJI-RES_266_XCVIII-O-21.pdf (oas.org), consulta realizada el 12 de mayo de 2021.

[371] Referencia en http://www.oas.org/es/sla/ddi/boletines_informativos_CJI_Principios_Actualizados_sobre_Privacidad_Proteccion_Datos_Personales_Abril-2021.html

El señalado anexo entrega una explicación detallada de los Principios, la que tiene por objeto proporcionar una guía para orientar la reflexión al interior de cada Estado Miembro de la OEA sobre su normativa en la materia, así como, cuando corresponda, reconocer en su caso los esfuerzos de fortalecimiento de estas.

Los Estados Miembros deberán determinar la forma en que se incorporan en sus respectivos ordenamientos jurídicos internos estos Principios, ya sea por medio de leyes, normas de naturaleza reglamentaria u otros mecanismos. Tales Estados deberían establecer reglas efectivas para la protección de Datos Personales que hagan eficaz el derecho de la persona a la privacidad y al respeto de sus Datos Personales, tutelando simultáneamente que la persona pueda beneficiarse del libre flujo de información y del acceso a la economía digital. Sin perjuicio de lo cual los Estados podrían ofrecer mecanismos adicionales para garantizar la privacidad y la protección de los Datos Personales, teniendo en cuenta las funciones y las finalidades legítimas para su Tratamiento en beneficio de las personas.

En lo que respecta al ámbito de aplicación de estos principios, que si bien no son vinculantes sino que constituyen, al igual que las recomendaciones de la Red Iberoamericana de Protección de Datos normas de *soft law*, destaca su regulación sobre los sectores públicos y privados, esto es, tanto sobre los datos personales generados, recopilados o administrados por entidades públicas como sobre los datos recopilados y tratados por entidades privadas que se encuentren en cualquier soporte físico o digital.

Los Principios no se aplican a los Datos Personales utilizados por una persona exclusivamente en el contexto de su vida privada, familiar o doméstica. Tampoco se aplican a la información anónima, es decir, aquella que no guarde relación con una persona física identificada o identificable, así como a los Datos Personales que han sido seudonimizados o sujetos a un proceso de Anonimización de tal forma que el Titular no pueda ser identificado o re identificado.

Los Principios tienen un carácter transversal estando relacionados entre sí, debiendo interpretarse en conjunto, con una perspectiva de género y de derechos humanos que identifique los impactos diferenciados del tratamiento de datos y los haga visibles para que tanto los Responsables como los Encargados de los datos personales puedan tomar las medidas necesarias para mitigar estas disparidades e impedir que el tratamiento menoscabe la dignidad y la privacidad de las personas que enfrentan situaciones de especial vulnerabilidad.

El Informe del Comité Jurídico Interamericano (CJI), en el apartado II, luego de la enumeración y descripción general de los principios, se refiere a una serie de definiciones, para a continuación profundizar en el contenido y alcance de cada uno de los principios que se analizan a continuación.

Principio Uno: Finalidades Legítimas y Lealtad

Los datos personales deberían ser recopilados solamente para finalidades legítimas y por medios leales y legítimos.

Estas nociones de legitimidad y lealtad deberían estar presentes desde la recopilación de los datos y durante todas las fases de su tratamiento, esto es en la recopilación, compilación, almacenamiento, utilización, divulgación y eliminación.

Sobre las finalidades legítimas estos principios señalan;

> *"Los Estados Miembros deberían, por lo tanto, incluir en sus legislaciones nacionales disposiciones específicas sobre las finalidades legítimas del Tratamiento de Datos Personales. Como regla general, estos podrían incluir casos en los que: (a) el Titular de los Datos otorgue su consentimiento expreso para el Tratamiento de sus Datos Personales para una o varias finalidades específicas; (b) el Tratamiento sea necesario para la ejecución de un contrato en el que el interesado es parte o para la aplicación a petición de éste de medidas precontractuales; (c) el Tratamiento sea necesario para el cumplimiento de una obligación legal aplicable al Responsable de datos; (d) el Tratamiento sea necesario para proteger intereses vitales del Titular o de otra persona; (e) el Tratamiento sea necesario para el cumplimiento de una misión realizada en interés público o en ejercicio de poderes públicos conferidos al Responsable de Datos; (f) el Tratamiento sea necesario para la satisfacción de intereses legítimos perseguidos por el Responsable de Datos; (g) el Tratamiento sea necesario para el cumplimiento de una orden judicial, resolución o mandato fundado y motivado de autoridad pública competente; y (h) el Tratamiento sea necesario para el reconocimiento o defensa de los derechos del Titular ante una autoridad pública".*

Como se puede apreciar las finalidades o propósitos en el tratamiento de datos deben sujetarse a determinados estándares como son; el consentimiento de su titular para el cumplimiento de uno o más fines; porque así se dispone en determinadas cláusulas contractuales o precontractuales de las que es parte o concurre el titular de los datos; porque se deriva de un mandato legal que recae sobre el responsable de los datos; porque el tratamiento tutela intereses esenciales para el titular de los datos o para otras personas; por razones de interés público, atribuciones otorgadas o satisfacción de legítimos intereses del responsable de los datos; por mandato debidamente fundado de una autoridad pública o jurisdiccional,; o para proteger y reconocer los derechos del titular de los datos ante una autoridad pública.

Y, sobre la lealtad agregan;

> *La "lealtad" es contextual y depende de las circunstancias. Requiere, entre otras cosas, que se ofrezcan opciones apropiadas a las personas con respecto a la forma y el momento en que vayan a proporcionar sus Datos Personales a los Responsables de los Datos en los casos en que no sea razonable prever que puedan recopilarse en vista de la relación de las personas con el recopilador o Encargado de Datos, y del aviso o los avisos que hayan recibido en el momento en que se recopilaron sus Datos. Las opciones que se ofrezcan a las personas no deberían interferir en las actividades y en la obligación de los Responsables de Datos de promover la seguridad externa e interna y el cumplimiento de la normativa ni impedir que empleen prácticas comúnmente aceptadas para la recopilación y utilización de Datos Personales.*

Esta noción de lealtad en el tratamiento de los datos personales, es circunstancial al contexto en el que se produce el tratamiento, constituyendo también un acto de confianza o *intuito personae* entre el titular de los datos, el responsable del tratamiento y el recopilador o encargado de los datos.

Principio Dos: Transparencia y Consentimiento

Este principio significa que en el momento anterior o durante la recogida de los datos *"se deberían especificar la identidad y datos de contacto del responsable de los datos, las finalidades específicas para las cuales se tratarán los datos personales, el fundamento jurídico que legitima su tratamiento, los destinatarios o categorías de destinatarios a los cuales los datos personales les serán comunicados, así como la información a ser transmitida y los derechos del titular en relación con los datos personales a ser recopilados"*[372]. Esa información que se transmite a la persona de la que se recaban los datos debe permitir un consentimiento "previo, inequívoco, libre e informado"[373]. De otra forma el consentimiento estaría viciado y sería a nuestro juicio, nulo.

En este sentido el consentimiento está vinculado a la transparencia sobre cómo se va proceder en el tratamiento de los datos personales. En concreto, el titular de los datos personales debe estar perfectamente informado sobre quien recopila (recoge o toma los datos) los datos, para qué se recogen (finalidad), así quien va a proporcionar esos datos y a quienes se van a ceder los datos. A ello se añade que al titular de los datos debe informársele sobre los derechos que le asisten según la legislación nacional (los derechos ARCO y derivados).

Principio Tres: Pertinencia y Necesidad

"Los datos personales deberían ser únicamente los que resulten adecuados, pertinentes, y limitados al mínimo necesario para las finalidades específicas de su recopilación y tratamiento ulterior". La pertinencia y la necesidad son principios cruciales de la protección de datos y la privacidad personal. Desde luego, sus requisitos deberían evaluarse en relación con el contexto específico en el cual se recopilen y ulteriormente traten. Las consideraciones contextuales incluyen qué datos particulares se recopilan y con qué finalidades y si son necesarios para alcanzarla.

La pertinencia implica que los datos deben tener una relación plausible con los fines para las cuales fueron recopilados y se tenga la intención de usarlos.

Los conceptos de "necesidad" y "proporcionalidad" imponen limitaciones generales al uso, lo cual significa que los datos personales solo deberían usarse para cumplir los propósitos de la recopilación, excepto con el consentimiento de la persona cuyos datos personales se recopilen o cuando sea necesario para proporcionar un producto o servicio solicitado por la persona.

Además, se debe reconocer que el tratamiento de datos está evolucionando continuamente desde el punto de vista tecnológico y, en consecuencia, este principio debe aplicarse con flexibilidad y adaptabilidad.

---

[372] OEA (2021) CJI/RES. 266 (XCVIII/21) de 9 de abril de 2021. *Principios actualizados sobre la privacidad y la protección de datos personales, con anotaciones.* https://www.informatica-juridica.com/etiqueta/derecho-informatico-oea/

[373] *Ibidem*

No creemos que la necesidad tenga que pasar por que sean datos imprescindibles, bastaría que se estimase que podrían ser necesarios dentro de una lógica y, siempre que no existiera desproporcionalidad.

Principio Cuatro: Tratamiento y Conservación Limitados.

La limitación en el tratamiento y conservación de los datos personales implica un tiempo tasado. *"Los datos personales deberían ser tratados y conservados solamente de manera legítima con las finalidades para las cuales se recopilaron" Y su "conservación no debería exceder del tiempo necesario para cumplir dichas finalidades y de conformidad con la legislación nacional correspondiente"*.

En este Principio se enuncian dos premisas fundamentales con respecto al tratamiento y la conservación de datos personales: 1) los datos deberían ser tratados y conservados solamente de una manera legítima que no sea incompatible con la finalidad para la cual se hayan recopilado, esto es lo que se denomina el "principio de finalidad" o de "limitación de la finalidad" y 2) no deberían conservarse más del tiempo necesario para cumplir su finalidad y de conformidad con la legislación nacional correspondiente.

Por ejemplo, cuando una persona da su nombre y su dirección a un vendedor en línea y dicho vendedor, a su vez da el nombre del titular y su domicilio particular al expedidor para que se puedan entregar al comprador los productos comprados, esa divulgación es evidentemente un uso "compatible" de datos personales. Sin embargo, si el vendedor da el nombre del titular y su domicilio particular a otro tipo de vendedor o comerciante con fines que no sean necesarios para completar la transacción en línea del titular y que no estén relacionados con dicha transacción, lo más probable es que sea un tratamiento "incompatible" de los datos del titular y que no estaría permitido salvo que el titular de los datos diera su consentimiento expreso. El tratamiento ulterior de datos personales con fines archivísticos, investigación científica e histórica o con fines estadísticos, todos ellos, en favor del interés público, no se consideraría incompatible con las finalidades iniciales. No obstante, dicho tratamiento ulterior seguiría sujeto a este principio de limitación en el tratamiento y la conservación de los datos. Así, otro caso en el cual este Principio podría aplicarse de manera razonable y con un alto grado de flexibilidades es el del uso de los datos personales de una persona como parte de un Tratamiento más amplio (o "agregado") de datos de un gran número de personas por el Responsable de datos; por ejemplo, para la elaboración de inventarios o con fines estadísticos o de contabilidad.

Igualmente, un Responsable de datos podría tener razones legales legítimas para conservarlos durante un período mayor al requerido; esto puede darse, por ejemplo, para cumplir otras obligaciones legales –de derecho nacional o internacional– o contractuales, o bien para proteger los derechos, la seguridad o los bienes de la persona del Encargado de los datos o de un tercero. Por ejemplo, los empleadores podrían conservar expedientes de exempleados o los médicos podrían conservar expedientes de ex-pacientes a fin de protegerse de ciertos tipos de acción judicial, como juicios por negligencia médica, despido ilegal, etc.

De lo anterior se colige que el tratamiento y conservación de los datos debe ser legítimo y cumplir una finalidad, es decir realizarse el tratamiento y perdurar con la información o data que ha sido tratada implica tener fundamentos jurídicos y facticos que los justifiquen.

Para salvaguardar este principio resulta fundamental la consagración y adecuada regulación de los denominados derechos ARCO, especialmente los referidos al de cancelación, supresión u olvido, principalmente en los entornos digitales y al de oposición.

Principio Cinco: Confidencialidad.

"Los datos personales no deberían divulgarse, ponerse a disposición de terceros, ni emplearse para otras finalidades que no sean aquellas para las cuales se recopilaron, excepto con el consentimiento de la persona en cuestión o bajo autoridad de la ley". Se trata del uso interno de los datos personales, al que solo deben tener acceso las personas que precisen su uso. Vedando el acceso a terceros o incluso a personas de la propia organización que no precisen el uso de los datos.

Es importante consignar eso sí, que la divulgación de datos personales a las autoridades encargadas de hacer cumplir la ley y a otras agencias gubernamentales, cuando sea realizada de conformidad con la legislación nacional, no contravendría este Principio, pero en todo caso la legislación nacional debería autorizarlo por medio de disposiciones claras y específicas. Tampoco se aplicaría la confidencialidad cuando se trate del propio titular de los datos personales.

Nuevamente aparecen como estándares para el adecuado tratamiento de los datos personales las nociones de finalidad, consentimiento y licitud. En efecto, el acceso a la información o data del titular es restrictivo y las causales que justifiquen su divulgación o apertura deben estar reguladas de manera previa en las legislaciones del respectivo país.

Principio Seis: Seguridad de los Datos.

La confidencialidad antes citada junto con la protección de los datos para evitar que sean alterados precisa de un sistema de seguridad. "*La confidencialidad, integridad y disponibilidad de los datos personales deberían ser protegidas mediante salvaguardias de seguridad técnicas, administrativas u organizacionales razonables y adecuadas contra tratamientos no autorizados o ilegítimos, incluyendo el acceso, pérdida, destrucción, daños o divulgación, aun cuando éstos ocurran de manera accidental. Estos mecanismos de resguardo deberían ser objeto de auditoría y actualización permanente"*. Los responsables de los datos deben establecer mecanismos técnico-administrativos para tutelar la seguridad de la información y data que será tratada, asegurando su reserva, coherencia y mantenimiento, estableciendo medidas que permitan disponer de la misma cuando esta se encuentre en su poder o bajo su resguardo. La seguridad de los datos debe considerar aspectos tales como: a) los derechos de los titulares de los datos; b) los costos de implementación de las medidas técnico-administrativas; c) el propósito o finalidad del tratamiento; y d) el tipo de datos personales que se traten, por ejemplo, si son o no datos sensibles.

Principio Siete: Exactitud de los Datos.

"Los datos personales deberían mantenerse exactos, completos y actualizados hasta donde sea necesario para las finalidades de su tratamiento, de tal manera que no se altere su veracidad".

La exactitud y la precisión revisten una importancia vital para la protección de la privacidad. Los datos inexactos pueden perjudicar tanto al Encargado de datos como al Titular, pero en una medida que varía mucho según el contexto.

La exactitud de la data es una directriz fundamental para mantener la debida integridad de la información que está siendo tratada, permitiendo que éste cumpla su propósito y no se modifique la verosimilitud de la misma. Este principio se encuentra intrínsecamente vinculado con los derechos de acceso y rectificación que permiten a su titular conocer la información que se está tratando, distinguiendo si esta es o no errónea e integra, ejercitando las acciones correctivas en caso de que existan errores o inexactitudes.

Principio Ocho: Acceso, Rectificación, Cancelación, Oposición y Portabilidad.

Este principio plantea los derechos ARCO de la protección de datos al que se añade la portabilidad, tal como lo hace el RGPD. Por parte de la OEA se indica que "*se debería disponer de métodos razonables, ágiles, sencillos y eficaces para permitir que aquellas personas cuyos datos personales han sido recopilados puedan solicitar el acceso, rectificación y cancelación de sus datos, así como el derecho a oponerse a su tratamiento y, en lo aplicable, el derecho a la portabilidad de esos datos personales. Como regla general, el ejercicio de esos derechos debería ser gratuito. En caso de que fuera necesario restringir los alcances de estos derechos, las bases específicas de cualquier restricción deberían especificarse en la legislación nacional y estar en conformidad con los estándares internacionales aplicables"*.

Estos derechos, también conocidos como derechos ARCO son acciones de tutela o mecanismos de garantía que conforman el núcleo esencial del derecho a la protección de datos siendo su ejercicio inherente al mismo.

Las personas deberían tener derecho a saber si los responsables de datos tienen información personal relacionada con ellas. Deben tener acceso a esos datos a fin de que puedan impugnar su exactitud y pedir al Responsable que modifique, revise, corrija o elimine los datos en cuestión. Estos derechos de acceso y rectificación son una de las salvaguardias más importantes en el campo de la protección de la privacidad. Las personas deben también tener derecho a cancelar sus datos personales, a objetar su tratamiento, y cuando sea aplicable, a la portabilidad de sus datos.

Como se analizará en las siguientes líneas, las legislaciones latinoamericanas más recientes han incorporado en sus respectivos ordenamientos jurídicos el derecho a la portabilidad, lo que implica solicitar al responsable o encargado del tratamiento un dispositivo que almacene su información tratada de la cual el titular pueda disponer libremente o, incluso que sus datos sean transferidos a un tercero.

Sus elementos esenciales son: i) la capacidad de la persona para obtener datos relacionados con ella en un plazo razonable y de una forma razonable e inteligible; para saber si se ha denegado una solicitud de acceso a dichos datos y por qué; y ii) la capacidad de impugnar tal denegación. Como regla general, el ejercicio de esos derechos debería ser gratuito; excepcionalmente, los costos deberían ser solamente aquellos asociados por razones naturales de reproducción, envío o certificación de los datos.

Como se verá más adelante, en algunos países de las Américas se reconoce el derecho de habeas data, en virtud del cual las personas pueden entablar juicio para prevenir un presunto abuso de sus datos personales o ponerle fin. Ese derecho podría dar a la persona acceso a bases de datos públicas o privadas, así como el derecho a corregir los datos en cuestión, a mantener el carácter confidencial de los datos personales sensibles y a rectificar o borrar datos perjudiciales. Como el contorno específico de este derecho varía de un Estado Miembro a otro, en estos Principios se abordan las cuestiones que plantea desde el punto de vista de cada uno de sus elementos, pero es la respectiva legislación nacional de cada Estado la que debería establecer los requerimientos, plazos, términos y condiciones en que los Titulares podrán ejercer los derechos de acceso, rectificación, cancelación, oposición y portabilidad, así como las causales de improcedencia al ejercicio de los mismos.

Estos derechos no son absolutos, y las legislaciones nacionales deberían especificar claramente las causas y razones por las cuales puede ser improcedente su ejercicio. Tales causales podrían incluir, de manera enunciativa mas no limitativa: 1) cuando el tratamiento sea necesario para el cumplimiento de un objetivo importante de interés público o para el ejercicio de las funciones propias de las autoridades públicas; 2) cuando el responsable acredite tener motivos legítimos para que el tratamiento prevalezca sobre los intereses, los derechos y las libertades del titular; 3) cuando el tratamiento sea necesario para el cumplimiento de una disposición legal; o 4) cuando los datos personales sean necesarios para el mantenimiento o cumplimiento de una relación jurídica o contractual.

Principio Nueve: Datos Personales Sensibles.

"Algunos tipos de datos personales, teniendo en cuenta su sensibilidad en contextos particulares, son especialmente susceptibles de causar daños considerables a las personas si se hace mal uso de ellos. Las categorías de estos datos y el alcance de su protección deberían indicarse claramente en la legislación y normativas nacionales. Los responsables de los datos deberían adoptar medidas de privacidad y de seguridad reforzadas que sean acordes con la sensibilidad de los datos y su capacidad de hacer daño a los titulares de los datos"[374].

Los "datos personales sensibles" son aquellos que se refieren a los aspectos más íntimos de las personas. Estos datos merecen protección especial porque, si se manejan o se divulgan de manera indebida, darían lugar a una intrusión profunda en la dignidad personal, el honor de la persona afectada y sus libertades fundamentales, y podrían desencadenar una discriminación ilícita o arbitraria contra la persona o causar un riesgo de graves perjuicios para la persona. Los

[374] Los entrecomillados de los principios corresponde a OEA (2021) CJI/RES. 266 (XCVIII/21) de 9 de abril de 2021. *Principios actualizados sobre la privacidad y la protección de datos personales, con anotaciones.* https://www.informatica-juridica.com/etiqueta/derecho-informatico-oea/

Estados Miembros deberían indicar claramente en su legislación y normativa nacionales las categorías de datos personales que se consideren especialmente "sensibles" y que, por consiguiente, requieran una mayor protección.

En efecto, la mayoría de las legislaciones iberoamericanas consagran los denominados datos sensibles, a modo de ejemplo la aún vigente regulación chilena, contenida en la ley N° 19.628 sobre protección a la vida privada dispone en su artículo 2° letra g): "g) Datos sensibles, [son] aquellos datos personales que se refieren a las características físicas o morales de las personas o a hechos o circunstancias de su vida privada o intimidad, tales como los hábitos personales, el origen racial, las ideologías y opiniones políticas, las creencias o convicciones religiosas, los estados de salud físicos o psíquicos y la vida sexual".

Existe una variedad de aproximaciones a estas categorías entre los Estados Miembros de la OEA, según el contexto cultural, social o político, podría incluir, por ejemplo, los datos relacionados con su salud personal, vida sexual, orientación sexual, creencias religiosas, filosóficas o morales, afiliación sindical, datos genéticos, datos biométricos dirigidos a identificar de manera univoca a una persona física, opinión política u origen racial o étnico, información sobre cuentas bancarias, documentos oficiales, información recopilada de niños y niñas o geolocalización personal.

Es decir, será cada país de acuerdo a sus concepciones culturales, sociales, políticas, económicas o incluso relacionadas con su idiosincrasia el que determinará que data o información es considerada sensible y por consiguiente objeto de una mayor restricción y resguardo.

Como regla general, los Datos Personales Sensibles no deberían ser tratados excepto, por ejemplo, cuando el Titular haya otorgado consentimiento expreso para ello o cuando el Tratamiento sea estrictamente necesario para el ejercicio y cumplimiento de las atribuciones y obligaciones específicas del Responsable de Datos o, para dar cumplimiento a un mandato legal, o razones de seguridad nacional, seguridad pública, orden público, salud pública, o salvaguarda de derechos y libertades de terceros. A manera de ejemplo, la necesidad de protección contra una amenaza transfronteriza grave a la salud pública, como sería una pandemia, podría quedar comprendida en estos supuestos. Al determinar las obligaciones reglamentarias pertinentes, hay que tener en cuenta el contexto en el cual una persona proporciona esos datos sensibles, el tipo de consentimiento y la finalidad en el tratamiento de los datos.

Si bien en su artículo 4° el RGPD de la UE no define los datos sensibles, si se regulan en el artículo 9.1 del Reglamento que señala: *"Quedan prohibidos el tratamiento de datos personales que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, y el tratamiento de datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud o datos relativos a la vida sexual o las orientación sexuales de una persona física".*

Principio Diez: Responsabilidad.

"Los responsables y encargados del tratamiento de datos deberían adoptar e implementar medidas técnicas y organizacionales que sean apropiadas y efectivas para asegurar y poder demostrar que el tratamiento se realiza en conformidad con estos Principios. Dichas medidas

deberían ser auditadas y actualizadas periódicamente. El responsable o encargado del tratamiento y, en lo aplicable, sus representantes, deberían cooperar, a petición, con las autoridades de protección de datos personales en el ejercicio de sus tareas".

Los sistemas de protección de la privacidad deberían reflejar un equilibrio apropiado entre la reglamentación gubernamental y la implementación ética y efectiva para aquellos que tienen responsabilidad directa por la recopilación, procesamiento, uso, retención y difusión de datos personales. Estos "responsables del tratamiento de datos personales" deberían actuar en calidad de "buen custodio" de los datos que les proporcionen o confíen y, además deberán cumplir con las responsabilidades que le atribuyan las normas que van desde dar satisfacción a los titulares de los datos de sus demandas de acceso, rectificación, cancelación, oposición, portabilidad; además de cumplir con los requerimientos de la autoridad de control, incluso con indemnizaciones por actos contrarios a la legalidad que generen daños y perjuicios.

La adhesión a códigos de conducta o mecanismos de certificación, entre otros, pueden usarse como elementos para demostrar cumplimiento con estos Principios o, al menos la presunción de buena fe. Por lo tanto, las leyes y normas nacionales en materia de privacidad deberían proporcionar una orientación claramente expresada y bien definida a los responsables en el tratamiento de datos, incluyendo la exigencia de que rindan cuentas del cumplimiento de estos Principios. Además del mecanismo con que cuenten las autoridades gubernamentales para hacer cumplir la normativa, el derecho interno debería proveer a las personas los mecanismos apropiados para comprometer a los responsables de los datos de las afectaciones que se produzcan.

Este principio sigue la máxima jurídica de que "quien cause un daño o perjuicio debe responder por ello", el régimen de responsabilidad al que estará afecto el encargado del tratamiento dependerá del ordenamiento jurídico interno del respectivo Estado miembro, lo relevante es que existan mecanismos que permitan certificar que el tratamiento siguió la directrices establecidas, siendo tal vez el más relevante el establecimiento de una autoridad de control en la materia que verifique y pueda hacer efectiva la responsabilidad en caso de incumplimiento.

Principio Once: Flujo Transfronterizo de Datos y Responsabilidad.

La tensión entre la necesaria transferencia de información a nivel mundial que incluye datos personales y la protección del derecho a la protección de datos, implica un esfuerzo de los países para conciliar ambos. Por ello en la citada Resolución 266 se dice que *"reconociendo su valor para el desarrollo económico y social, los Estados Miembros deberían cooperar entre sí para facilitar el flujo transfronterizo de datos personales a otros Estados cuando estos confieran un nivel adecuado de protección de los datos de conformidad con estos Principios. Asimismo, los Estados Miembros deberían cooperar en la creación de mecanismos y procedimientos que aseguren que los responsables y encargados del tratamiento de datos que operen en más de una jurisdicción, o los transmitan a una jurisdicción distinta de la suya, puedan garantizar y ser efectivamente hechos responsables por el cumplimiento de estos Principios"*.

En este aspecto la citada Resolución 266 del Comité Jurídico Interamericano (CJI) señala que *"en el mundo moderno de rápidos flujos de datos y comercio transfronterizo, es cada vez más probable que las transferencias de Datos Personales crucen fronteras nacionales. Sin*

embargo, la reglamentación que existe actualmente en diversas jurisdicciones nacionales varía en cuanto al fondo y al procedimiento. En consecuencia, existe la posibilidad de confusión, conflictos y contradicciones, por lo cual es deseable que los Estados Miembros de la OEA consideren reconocer estándares interoperables para transferencias transfronterizas de datos personales".

"Un reto fundamental para una política y una práctica eficaces en materia de protección de Datos consiste en conciliar 1) las diferencias en los enfoques nacionales de la protección de la privacidad con la realidad moderna del flujo mundial de Datos; 2) los derechos de las personas a tener acceso a Datos en un contexto transnacional; y 3) el hecho fundamental de que los Datos y el Tratamiento de Datos impulsan el desarrollo y la innovación. Todos los instrumentos internacionales para la protección de Datos procuran alcanzar un equilibrio apropiado entre esas metas.

"En estos Principios se expresa una directriz para que cada Estado Miembro de la OEA evalúe sus propios mecanismos de protección de la privacidad de cara al flujo transfronterizo de datos personales. Al igual que en otras normas internacionales en este campo, en estos Principios se adopta una norma de razonabilidad con respecto a las transferencias transfronterizas. Por una parte, deberían permitirse las transferencias internacionales de Datos Personales entre Estados Miembros que confieran los grados de protección reflejados en estos Principios o que protejan los Datos Personales en medida suficiente por otros medios, entre ellos mecanismos efectivos de aplicación de la normativa. Al mismo tiempo, deberían permitirse las transferencias también en los casos en que los mismos Responsables de Datos tomen medidas apropiadas para asegurar que los Datos transferidos estén protegidos de manera efectiva en consonancia con estos Principios. Los Estados Miembros deberían tomar las medidas necesarias para que los Responsables y Encargados de Datos se responsabilicen de esa protección".

Este principio hay que entenderlo desde la perspectiva que a nivel latinoamericano, a diferencia de lo que ocurre en la Unión Europea, no existe un instrumento de regulación común de carácter vinculante que estandarice el tratamiento de datos de carácter personal en cada uno de los Estados de la región, por ello directrices contenidas en estos principios, así como los estándares propuestos por la Red Iberoamericana de protección de datos constituyen una guía o camino a seguir en la materia, que los Estados latinoamericanos deberían considerar.

Principio Doce: Excepciones.

"Cualquier excepción a alguno de estos Principios debería estar prevista de manera expresa y específica en la legislación nacional, ser puesta en conocimiento del público y limitarse únicamente a motivos relacionados con la soberanía nacional, la seguridad nacional, la seguridad pública, la protección de la salud pública, el combate a la criminalidad, el cumplimiento de normativas u otras prerrogativas de orden público, o el interés público".

Estas excepciones y desviaciones respecto de la norma deberían ser la excepción y no la regla, aplicándose solo después de considerar lo más cuidadosamente posible la importancia de proteger la privacidad individual, la dignidad y el honor, respetando los derechos y las libertades fundamentales de los Titulares. Debería haber límites sensatos en la capacidad de las autoridades nacionales para compeler a los Responsables a dar a conocer datos personales,

manteniendo un equilibrio entre la necesidad de los datos en circunstancias limitadas y el debido respeto al derecho de los intereses de las personas en materia de privacidad.

Debería introducirse una ponderación que incluyera las pruebas del daño y del interés público. Esto es, determinar cuánto daño se produciría si se aplica la excepción, tanto en el titular de los datos personales como en el bien jurídico que concurre en la excepción (seguridad nacional, protección de la salud….) la prueba del interés público determinaría la afectación mayor o menor a toda la población.

Esta directriz de excepcionalidad, como su nombre lo indica, no puede ni debe constituir un espacio para la ambigüedad, ni menos para la arbitrariedad de parte de la autoridad de control del respectivo Estado miembro. La premisa debe ser proteger la privacidad, data e información de los titulares del derecho a la protección de datos personales, pudiendo ser tal derecho única y exclusivamente alterado por causas de excepción debidamente motivadas (desde el punto de vista normativo y factico) previamente establecidas en la normativa respectiva.

Principio Trece: Autoridades de Protección de Datos.

Este Principio viene a establecer que *"los Estados Miembros deberían establecer órganos de supervisión independientes, dotados de recursos suficientes, de conformidad con la estructura constitucional, organizacional y administrativa de cada Estado, para monitorear y promover la protección de datos personales de conformidad con estos Principios. Los Estados Miembros deberían promover la cooperación entre tales órganos"*[375].

Este principio resulta de suma importancia para el desarrollo de esta investigación doctoral, por cuanto se estima indispensable el establecimiento de una Autoridad de Control que promueva y regule la protección de datos personales constituyéndose como un mecanismo de tutela y garantía de este derecho fundamental, además de difusión y promoción del derecho.

En virtud de este principio se promueve que la mayoría de los Estados Miembros de la OEA establezcan organismos reguladores nacionales autónomos, que se encarguen de establecer y hacer cumplir leyes, normas y requisitos relativos a la protección de datos personales, promuevan el derecho a la protección de datos y se coordinen con el objeto de lograr un sistema lo más uniforme posible.

Ahora bien, los parámetros para el establecimiento de una Autoridad de Control en cada país variarán dependiendo de diversos factores, sin embargo resulta esencial que esta entidad de la respectiva administración pública tenga un carácter técnico y especializado, además de contar con la debida autonomía o independencia del gobierno de turno, para la regulación y promoción de la protección de datos y este dotada de las competencias y recursos necesarios para ello.

Sin embargo, como no se observa un enfoque uniforme en la región, cada Estado Miembro de la OEA deberá abordar individualmente la naturaleza específica, la estructura, las autoridades y las responsabilidades de estas Autoridades Responsables de la Protección de Datos. La

[375] Los entrecomillados de los principios corresponden a OEA (2021) CJI/RES. 266 (XCVIII/21) de 9 de abril de 2021. *Principios actualizados sobre la privacidad y la protección de datos personales, con anotaciones.* https://www.informatica-juridica.com/etiqueta/derecho-informatico-oea

legislación nacional de cada Estado debería dotar a dichas autoridades de la capacidad de cooperar internacionalmente entre sí, así como con las instituciones públicas y privadas relevantes, incluyendo las relacionadas al ámbito penal, financiero, del consumidor, entre otras, cuyas labores tengan relación o incidencia con la protección de datos personales.

Se insta a los Estados Miembros a que establezcan disposiciones, procedimientos o instituciones jurídicas, administrativas y de otros tipos que sean apropiados y eficaces para proteger la privacidad y las libertades individuales con respecto a los datos personales. Los Estados miembros deberían crear medios razonables para que las personas ejerzan sus derechos fomenten y apoyen la autorregulación (con códigos de conducta o por otros medios) de los Responsables de datos y los Encargados de datos. Asimismo, deberían establecer sanciones y recursos adecuados para los casos de incumplimiento, cerciorándose además de que no se discrimine injustamente a los Titulares de los datos. Los Estados Miembros deberían establecer también los requisitos mínimos para cualquier tipo de protección de datos que las autoridades escojan, a fin de proporcionarles los recursos, el financiamiento y la pericia técnica que necesiten para desempeñar sus funciones de manera eficaz.

La Protección de datos en Estados Unidos

Antes de abordar la regulación de la protección de datos en Latinoamérica, parece pertinente considerar cual es el sistema de regulación existente en uno de los países que más influye y desarrolla el intercambio comercial y, por consiguiente de datos, precisamente con América Latina, como es el caso de Estados Unidos.

El desarrollo de las nuevas tecnologías, así como el *big data* y las operaciones comerciales transnacionales representan un desafío, pero también una enrome oportunidad para Latinoamérica en relación con el desarrollo y regulación del derecho a la protección de datos, considerando los diferentes modelos o sistemas de regulación que existen en la región y que dan cuenta de una falta de uniformidad en la materia. La entrada en vigor del RGPD, como ya se ha señalado, ha contribuido a impulsar nuevas legislaciones que avancen en la regulación de la protección de datos, así como en la configuración de una autoridad de control, que efectivamente tutele ese derecho. La influencia del Reglamento ha sido mayor, a pesar de la distancia geográfica, que el modelo norteamericano de protección de datos, que como se verá a continuación responde más bien a una autorregulación de los responsables de los datos que además ofrecen un compromiso a sus clientes que van a proteger sus datos personales (una política de privacidad que se expresa en un documento a disposición del titular de los datos) completado en muchos casos con una auditoria externa[376] y, en último término a un mecanismo de tutela radicado en la judicatura.

[376] Por ejemplo, el programa de privacidad de BBOn line, que revisa las prácticas de privacidad de la empresa, como su sitio web utiliza las cookies, aunque también incluye cuestiones como la veracidad de la publicidad, el cumplimiento de una prácticas comerciales responsables, un compromiso de resolución de disputas y que la mneos ha estado un año en el negocio.

También podemos citar "TRUSTe Privacy Certification and Assurance Services" (Servicios de garantía y certificación de privacidad de TRUSTe" que vienen a demostrar "el cumplimiento de la privacidad, reduzca el

En efecto, en Estados Unidos no existe una Ley Federal de Protección de datos, quedando la regulación de esta materia radicada en leyes sectoriales y ámbitos contractuales específicos, como por ejemplo la *Fair Credit Reporting Act* de 1970, que es la Ley de Información Crediticia Imparcial, que promueve la imparcialidad y privacidad de la información financiera de los consumidores, como evaluaciones de crédito o informes de solvencia. O la *Equal Credit Opportunity* Act de 1974, que es la Ley de Igualdad de Oportunidades de Crédito, que impide la discriminación de las personas para que puedan acceder a operaciones crediticias por su color, raza, religión, nacionalidad, sexo, estado civil o edad. Como también la *Health Insurance Portability and Accountability Act* de 1996 que es la Ley de Portabilidad y Transferencia de Seguros Médicos, que persigue resguardar la información de salud de los pacientes, frente a las entidades de salud y aseguradoras.

También, pero como una afectación al derecho a la privacidad y a la protección de datos relacionada con la seguridad nacional, el 13 de mayo de 2020 el Senado de Estados Unidos, con 59 votos a favor, aprobó una modificación a la Sección 215 de la Ley Patriota, *Us Patriot Act*, por la cual se faculta a la CIA y al FBI para ingresar y vigilar los historiales de los navegadores de los usuarios de la red, en forma remota, sin orden judicial previa y sin acreditar causa probable, cuando se trata de prevenir, investigar o buscar sanciones para actos que pongan en peligro o atenten contra la Seguridad Nacional de Estados Unidos. Tanto la CIA como el FBI podrán usar esta nueva herramienta legal dentro de Estados Unidos como en sus acciones internacionales, precaviendo el interés norteamericano.

Con lo expuesto, es fácil advertir que el sistema norteamericano se focaliza más bien en la defensa de los consumidores y en las relaciones comerciales, que en la tutela a la protección de datos propiamente tal.

Eso sí, como señala Padín Vidal: "… esta situación puede cambiar en un plazo no muy largo, y ello debido a la presión de los consumidores, pero también las empresas que tratan datos están poniendo en la promulgación de una ley federal de protección de datos personales. Esa presión surge, principalmente, tras diversos acontecimientos acaecidos durante los años 2017 y 2018, relacionados tanto con las brechas de seguridad a gran escala en grandes empresas que disponían de gran número de datos (Equifax, Marriott…) como con tratamientos específicos realizados por empresas con cierta opacidad o desconocimiento por parte de los interesados (Cambridge Analytica).

Fruto de esta situación, en el ámbito federal se ha presentado el 1 de noviembre de 2018 un primer documento de trabajo para un anteproyecto de una futura ley de protección de datos que, bajo el nombre de *"Consumer Data Protection Act"*, vendría a reformar diversos aspectos de la *"Federal Trade Commission Act"* para introducir obligaciones y derechos en materia de tratamiento de datos personales. Ese documento de trabajo incluye obligaciones para algunas empresas como la de presentar un informe anual de protección de datos, u ofrecer la posibilidad

riesgo y genere confianza con una revisión independiente impulsada por la tecnología, realizada por expertos en privacidad" https://trustarc.com/truste-certifications/

Pueden consultarse las iniciativas de privacidad en https://trustarc.com/truste-certifications/

a los interesados de exigir a las empresas que no traten sus datos ("op-out") para diversas finalidades, tales como la cesión de los datos a terceros"[377].

El Modelo Estadounidense, se sustenta en la IV Enmienda, que dispone: *"El derecho de los habitantes de que su persona, domicilios, papeles y efectos se hallen a salvo de pesquisas y aprehensiones arbitrarias, será inviolable, y no se expandirán al efecto mandamientos que no se apoyen en un motivo verosímil, estén corroborados mediante juramento o protesta y describan con particularidad el lugar que deba ser registrado y las personas o cosas que han de ser detenidas o embargadas"*.

La IV Enmienda tiene larga data, requiere que las pesquisas y aprehensiones de la autoridad, y la invasión de la privacidad, estén revestidas de una "causa razonable" y tuvo su origen en la *Bill of Rights*, como respuesta a los abusos de la antigua "Orden General de Registro" de la Guerra de la Independencia.

En materia de acceso a documentos digitales y de datos informáticos en USA es necesario que la acción se ajuste a la Regla de Evidencia 34, sus criterios y Jurisprudencia. La Regla dice cómo proceder, y cuándo se permite acceder a documentos almacenados electrónicamente, a cosas tangibles, o situadas en tierra, para inspección y otros fines pertinentes a la investigación. Remite a la Regla 26 (b), que en síntesis fija el espectro posible de entrega de información o apertura de fuentes no sujetas a privilegio de reserva o secreto (Discovery), normalmente ejecutable por medio de una Moción[378].

Así entonces, como lo plantea Guerrero Picó, la privacidad solo se considera fundamental cuando se ve amenazada por un abuso gubernamental en el trato de la información personal y, por lo tanto, la ley federal interviene solo frente a él o, también, cuando se trata de negocios que almacenan información personal sensible. Salvadas estas circunstancias, la protección de los datos se considera un elemento disponible por parte de los ciudadanos[379].

Esta Enmienda hay que entenderla en armonía con la Primera de la Constitución de los Estados Unidos, que tutela la libertad de expresión y que por consiguiente limita a su vez la tutela del derecho a la privacidad[380]. En consecuencia, el modelo de protección de datos de ese país se configura sobre la idea de delimitar el ámbito personal que no puede ser invadido por el Estado, lo que desembocó en el año 1974 en la dictación del *Privacy Act*, que tiene un alcance limitado al tratamiento de datos del gobierno federal, sin perjuicio de la legislación estatal que se dicte en la materia, como el caso del Estado de California que se analizará en el siguiente apartado.

De lo expuesto, es posible distinguir dos grandes diferencias entre el modelo estadounidense y europeo en materia de protección de datos de carácter personal:

---

[377]Padin Vidal, A. (2019), "Protección de datos en Colombia, Perú, México y Brasil. Referencia a Estados Unidos", en *La Adaptación al nuevo marco de protección de datos tras el RGPD y la LOPDGDD*. Coordinador José López Clavo, Wolters Kluwer, pp. 1083-1084.

[378] Ver: https://www.law.cornell.edu/rules/frcp/rule_34.

[379] Guerrero Picó, M. C, (2006), "El Impacto del Internet en el derecho fundamental a la protección de datos de carácter personal", sine loco, Thomson Civitas, p.347.

[380] Señala la Primera Enmienda: "El Congreso no podrá hacer ninguna ley con respecto al establecimiento de la religión, ni prohibiendo la libre practica de la misma; ni limitando la libertad de expresión, ni de prensa; ni el derecho a la asamblea pacifica de las personas, ni de solicitar al gobierno una compensación de agravios".

1. El enfoque norteamericano se sustenta fundamentalmente en la noción de libertad como contrapartida a la intervención estatal en la vida de las personas, promoviendo principalmente la autorregulación.

2. El sistema europeo tiene un alcance más general y uniforme, que ha sido reforzado por el RGPD, donde se tutela y reconoce el derecho a la protección de datos por parte del Estado, el cual interviene activamente en su promoción y protección.

Hay autores como Villegas Carrasquilla, que plantean un tercer modelo, el latinoamericano, que se sustentaría en el derecho fundamental de *habeas data*, que además de ser un derecho fundamental, es una acción de protección de la que gozan los titulares de los datos, frente al tratamiento indebido o ilegal de los mismos, alojados en archivos de entidades tanto públicas como privadas[381]. Latinoamérica se diferencia del modelo europeo, fundamentalmente porque no existe una norma, tratado o instrumento multilateral (aparte de las regulaciones iberoamericanas de *soft law*, ya revisadas) de carácter general que regule la protección de datos de carácter personal.

Ley de Privacidad del Consumidor de California

El Reglamento europeo ha servido de inspiración para otras regulaciones relevantes en la materia, como es el caso de la Ley AB-375, que modifica el Código Civil de California, también denominada Ley de Privacidad del Consumidor de California, *California Consumer Privacy Act*[382] o CCPA, que entró en vigor el primero de enero del año 2020. Esta ley actualizó el régimen de protección de datos en dicho Estado adaptándose a las condiciones y requerimientos propios de la era digital, estableciendo entre otros, el derecho del consumidor a saber qué información personal es recolectada por las empresas, así como el derecho de oposición que tienen los titulares sobre la venta de sus datos[383].

Esta Ley fue aprobada en agosto de 2018, y se perfila como un referente en la legislación estadounidense, que se ha caracterizado siempre por una mayor laxitud con respecto al tratamiento de datos personales en relación con la regulación de la UE. Además de los derechos reconocidos a los consumidores, la CCPA incluye también obligaciones de las empresas, delimita los negocios que han de acogerse a esta ley y especifica las sanciones aplicables en caso de no atenerse a lo dispuesto en ella.

La CCPA busca delimitar el uso que hacen las empresas de los datos de los consumidores, otorgando a estos un mayor control sobre los mismos y aumentando la protección de su privacidad. De este modo, la CCPA reconoce el derecho de los consumidores a saber qué

[381] Villegas Carrasquilla, L. (2012), "Protección de datos personales en América Latina: retención y tratamiento de datos personales en el mundo de Internet", en *"Hacia una Internet Libre de Censura, Propuesta de América Latina"*, Facultad de Derecho, Centro de Estudios en Libertad de Expresión y Acceso a la Información, compilador Eduardo Bertoni, Buenos Aires, p.130.

[382]https://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?division=3.&part=4.&lawCode=CIV&title=1.81.5

[383] Un resumen de la Ley de California puede encontrarse en https://oag.ca.gov/privacy/ccpa

información recopilan las empresas sobre ellos, para qué propósito y con quién la comparten. Asimismo, los consumidores pueden pedir a las empresas la eliminación de sus datos personales, así como prohibirles su venta o divulgación a terceros. De hecho, las empresas deben mostrar en un lugar visible de su página web un enlace con la información *"Do Not Sell My Personal Information"* (no vender mi información personal), para que los consumidores puedan ejercer este derecho.

En definitiva, esta ley de privacidad ofrece a los consumidores mayor control sobre sus datos personales y les otorga el derecho a saber qué información personal se está recopilando sobre ellos, tanto por categoría como por datos específicos que las empresas hayan recopilado. En este mismo sentido, el derecho a saber si su información personal se está vendiendo o divulgando de otra manera y a quién. Todo lo cual es regulado por la Sección 8380 (b) (2) del Código de Servicios Públicos, que prohíbe vender datos de los clientes o su información de identificación personal.

Esta ley también reconoce el derecho a que la información personal se elimine en ciertas circunstancias, otorgando al titular el derecho a solicitar que la empresa elimine cualquier información personal suya que haya recopilado y conservado.

Si bien el CCPA no es una normativa nacional aplicable a todos los Estados Unidos, el impacto que esta tiene es significativo, considerando el tamaño de la población del Estado de California, con casi cuarenta millones de habitantes y la influencia que su economía tiene para el país del norte, sumado al hecho de que las grandes empresas de internet a nivel mundial tienen su sede en California, como es el caso de Facebook (ubicada en *Menlo Park*, California), Google (ubicada en *Mountain View*, California), Apple (ubicada en Cupertino, California), Netflix (ubicada en Los Gatos, California) y Twitter (ubicada en San Francisco, California), solo por mencionar algunas.

La Protección de Datos en las Constituciones Latinoamericanas

Tal vez uno de los aspectos distintivos de la regulación en materia de protección de datos sea su generalizado reconocimiento o tratamiento a nivel constitucional. En efecto, el reconocer el derecho a la protección de datos en las Cartas políticas latinoamericanas, aun cuando no sea explícitamente, es un proceso que se observa desde la década de los ochenta y que se extiende incluso hasta el presente siglo veintiuno, eso sí, la forma, contenido y alcance de este reconocimiento constitucional no es uniforme. A continuación, se analizará cómo se aborda constitucionalmente la protección de datos en los países de la región:

Argentina

En Argentina la protección de datos es un derecho que se deriva del artículo 43 de la Constitución, que regula fundamentalmente el recurso de amparo para tutelar la afectación de derechos y garantías constitucionales. Resultando especialmente relevante para este trabajo lo dispuesto en el inciso tercero, en el sentido de que esta acción tutela también la protección de datos de carácter personal que conste en registros o bases de datos públicos y privados,

consagrando además constitucionalmente los derechos de supresión, rectificación, confidencialidad y actualización, sobre los datos de que se es titular. Dispone el artículo 43:

> *"Toda persona puede interponer acción expedita y rápida de amparo, siempre que no exista otro medio judicial más idóneo, contra todo acto u omisión de autoridades públicas o de particulares, que en forma actual o inminente lesione, restrinja, altere o amenace, con arbitrariedad o ilegalidad manifiesta, derechos y garantías reconocidos por esta Constitución, un tratado o una ley. En el caso, el juez podrá declarar la inconstitucionalidad de la norma en que se funde el acto u omisión lesiva.*
> *Podrán interponer esta acción contra cualquier forma de discriminación y en lo relativo a los derechos que protegen al ambiente, a la competencia, al usuario y al consumidor, así como a los derechos de incidencia colectiva en general, el afectado, el defensor del pueblo y las asociaciones que propendan a esos fines, registradas conforme a la ley, la que determinará los requisitos y formas de su organización.*
> *Toda persona podrá interponer esta acción para tomar conocimiento de los datos a ella referidos y de su finalidad, que consten en registros o bancos de datos públicos, o los privados destinados a proveer informes, y en caso de falsedad o discriminación, para exigir la supresión, rectificación, confidencialidad o actualización de aquéllos. No podrá afectarse el secreto de las fuentes de información periodística.*
> *Cuando el derecho lesionado, restringido, alterado o amenazado fuera la libertad física, o en caso de agravamiento ilegítimo en la forma o condiciones de detención, o en el de desaparición forzada de personas, la acción de hábeas corpus podrá ser interpuesta por el afectado o por cualquiera en su favor y el juez resolverá de inmediato, aun durante la vigencia del estado de sitio".*

Bolivia

En Bolivia, la regulación constitucional a la protección de datos de carácter personal se encuentra contenida tanto en el artículo 21.2 que se refiere al derecho a la privacidad, intimidad, honra, honor, propia imagen y dignidad, como en el Capítulo Segundo sobre las "Acciones de Defensa", cuya Sección III se refiere a la Acción de Protección a la Privacidad, en la cual se contienen los artículos 130 y 131 de la Carta Política.

El artículo 130 dispone:

> *"Toda persona individual o colectiva que crea estar indebida o ilegalmente impedida de conocer, objetar u obtener la eliminación o rectificación de los datos registrados por cualquier medio físico, electrónico, magnético o informático, en archivos o bancos de datos públicos o privados, o que afecten a su derecho fundamental a la intimidad y privacidad personal o familiar, o a su propia imagen, honra y reputación, podrá interponer la Acción de Protección de Privacidad".*

Y luego del artículo 131 se refiere a los plazos y procedimiento general de la Acción de Protección a la Privacidad, al señalar:

> *". I. La Acción de Protección de Privacidad tendrá lugar de acuerdo con el procedimiento previsto para la acción de Amparo Constitucional. II. Si el tribunal o juez competente declara procedente la acción, ordenará la revelación, eliminación o rectificación de los datos cuyo registro fue impugnado. III. La decisión se elevará, de oficio, en revisión ante el Tribunal Constitucional Plurinacional en el plazo de las*

> *veinticuatro horas siguientes a la emisión del fallo, sin que por ello se suspenda su ejecución. IV. La decisión final que conceda la Acción de Protección de Privacidad será ejecutada inmediatamente y sin observación. En caso de resistencia se procederá de acuerdo con lo señalado en la Acción de Libertad. La autoridad judicial que no proceda conforme con lo dispuesto por este artículo quedará sujeta a las sanciones previstas por la ley".*

Brasil

La Constitución de Brasil[384], si bien no se refiere expresamente al derecho a la protección de datos personales, es posible de extraerlo del artículo 5, que aborda la igualdad ante la ley, al derecho a la vida, a la libertad y a la seguridad, y que en su numeral setenta y uno consagra el habeas data para asegurar el conocimiento de informaciones relativas a la persona del impetrante que consten en registros o bancos de datos de entidades gubernamentales o de carácter público y para la rectificación de datos, cuando no se prefiera hacerlo por procedimiento secreto, judicial o administrativo. Dispone el señalado numeral 71:

> *"Se concederá "habeas data": 1. para asegurar el conocimiento de informaciones relativas a la persona del impetrante que consten en registros o bancos de datos de entidades gubernamentales o de carácter público; 2. para la rectificación de datos, cuando no se prefiera hacerlo por procedimiento secreto, judicial o administrativo".*

Chile

Como ya se señaló en el capítulo primero, la Constitución chilena, a través de la Ley N° 21.096, publicada en el Diario Oficial el 16 de junio del año 2018, introdujo una modificación al numeral cuarto del artículo 19, consagrando expresamente el derecho a la protección de datos, al señalar:

> *"La Constitución asegura a todas las personas (…) 4° El respeto y protección a la vida privada y a la honra de la persona y su familia, y, asimismo, la protección de sus datos personales. El tratamiento y protección de estos datos se efectuará en la forma y condiciones que determine la ley".*

Estableciendo así un reconocimiento explícito al derecho fundamental a la protección de datos de carácter personal que, si bien se mantiene relacionado con el respeto y protección a la vida privada y la honra de las personas, adquiere una autonomía y configuración propia.

Colombia

La Constitución Colombiana en su artículo 15 dispone que:

> *"Todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, y el Estado debe respetarlos y hacerlos respetar. De igual modo, tienen*

[384] Es importante precisar que una vez concluida la presente investigación doctoral, el Congreso Nacional de Brasil promulgó el 10 de febrero de 2022 la enmienda constitucional 115, que incluye la protección de datos personales como un derecho fundamental de los brasileños previsto en la Constitución. El texto determina que la Unión debe "organizar y supervisar la protección y el tratamiento de los datos personales, de conformidad con la ley", incluso en medios digitales.

derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos y en archivos de entidades públicas y privadas.
En la recolección, tratamiento y circulación de datos se respetarán la libertad y demás garantías consagradas en la Constitución.
La correspondencia y demás formas de comunicación privada son inviolables. Sólo pueden ser interceptadas o registradas mediante orden judicial, en los casos y con las formalidades que establezca la ley".

Costa Rica

Por su parte, Costa Rica garantiza el derecho a la intimidad, a la libertad y al secreto de las comunicaciones, en su artículo 24, al señalar que:

"Son inviolables los documentos privados y las comunicaciones escritas, orales o de cualquier otro tipo de los habitantes de la República. Sin embargo, la ley, cuya aprobación y reforma requerirá los votos de dos tercios de los Diputados de la Asamblea Legislativa, fijará en qué casos podrán los Tribunales de Justicia ordenar el secuestro, registro o examen de los documentos privados, cuando sea absolutamente indispensable para esclarecer asuntos sometidos a su conocimiento. Igualmente, la ley determinará en cuáles casos podrán los Tribunales de Justicia ordenar que se intervenga cualquier tipo de comunicación e indicará los delitos en cuya investigación podrá autorizarse el uso de esta potestad excepcional y durante cuánto tiempo. Asimismo, señalará las responsabilidades y sanciones en que incurrirán los funcionarios que apliquen ilegalmente esta excepción. Las resoluciones judiciales amparadas a esta norma deberán ser razonadas y podrán ejecutarse de inmediato. Su aplicación y control serán responsabilidad indelegable de la autoridad judicial. La ley fijará los casos en que los funcionarios competentes del Ministerio de Hacienda y de la Contraloría General de la República podrán revisar los libros de contabilidad y sus anexos para fines tributarios y para fiscalizar la correcta utilización de los fondos públicos. Una ley especial, aprobada por dos tercios del total de los Diputados, determinará cuáles otros órganos de la Administración Pública podrán revisar los documentos que esa ley señale en relación con el cumplimiento de sus competencias de regulación y vigilancia para conseguir fines públicos. Asimismo, indicará en qué casos procede esa revisión. No producirán efectos legales, la correspondencia que fuere sustraída ni la información obtenida como resultado de la intervención ilegal de cualquier comunicación.
Para efectos tributarios o judiciales y para los casos de inspección, vigilancia e intervención del Estado podrá exigirse la presentación de libros de contabilidad y demás documentos privados, en los términos que señale la ley".

En Costa Rica tradicionalmente se ha entendido que el derecho a la protección de datos personales, al igual que en muchas otras legislaciones latinoamericanas, es un derecho dependiente y derivado de la intimidad, sin embargo, como ya se ha señalado, este es un derecho distinto y autónomo. Por lo que se impulsa una reforma al artículo 24, que fue presentada el pasado 30 de junio de 2020, como Proyecto de Reforma Constitucional,

singularizado con el expediente N° 22063[385] cuya finalidad es incluir el derecho a la protección de datos personales en el bloque constitucional de garantías individuales lo que permitiría que el ciudadano pueda intentar una acción de tutela ante el máximo nivel de la judicatura en la Sala Constitucional, la que podría realizar un control de constitucionalidad en la materia sobre la totalidad del ordenamiento jurídico, en especial en el proceso de formación de la ley.

Cuba

En el caso cubano, la Constitución de la República de Cuba fue aprobada por la Asamblea Nacional del Poder Popular, en el Segundo Período Ordinario de Sesiones de la IX Legislatura y ratificada en referendo popular el 24 de febrero de 2019. Esta consagra el derecho a la protección de datos en su artículo 97, y se ubica en el Capítulo VI de la Carta titulado "Garantías de los Derechos" y que por consiguiente otorgan una tutela judicial efectiva[386]. Dispone el artículo noventa y siete que:

> *"Se reconoce el derecho de toda persona de acceder a sus datos personales en registros, archivos u otras bases de datos e información de carácter público, así como a interesar su no divulgación y obtener su debida corrección, rectificación,*

[385] El texto propuesto en la Reforma es el siguiente: "Artículo 24. Se garantiza el derecho a la vida privada, a la protección de los datos personales, a la libertad y al secreto de las comunicaciones. Mediante ley especial podrán adoptarse limitaciones a estos derechos para salvaguardar la seguridad nacional, la seguridad pública, la protección de la salud pública, la protección de los derechos y las libertades de terceros, así como por cuestiones de interés público.

Son inviolables los documentos privados, los datos personales sensibles y las comunicaciones escritas, orales o de cualquier otro tipo de los habitantes de la República. Sin embargo, la ley, cuya aprobación y reforma requerirá los votos de dos tercios de los Diputados de la Asamblea Legislativa, fijará en qué casos podrán los Tribunales de Justicia ordenar el secuestro, registro o examen de los documentos privados, o datos personales sensibles, cuando sea absolutamente indispensable para esclarecer asuntos sometidos a su conocimiento.

Igualmente, la ley determinará en cuáles casos podrán los Tribunales de Justicia ordenar que se intervenga cualquier tipo de comunicación e indicará los delitos en cuya investigación podrá autorizarse el uso de esta potestad excepcional y durante cuánto tiempo. Asimismo, señalará las responsabilidades y sanciones en que incurrirán los funcionarios que apliquen ilegalmente esta excepción. Las resoluciones judiciales amparadas a esta norma deberán ser razonadas y podrán ejecutarse de inmediato. Su aplicación y control serán responsabilidad indelegable de la autoridad judicial.

Una ley especial, aprobada por dos tercios del total de los Diputados, fijará los casos en que los funcionarios competentes del Ministerio de Hacienda y de la Contraloría General de la República podrán revisar los sistemas de contabilidad y sus soportes, o acceder a datos personales para fines tributarios y para fiscalizar la correcta utilización de los fondos públicos, y cuáles otros órganos de la Administración Pública podrán revisar los documentos o acceder a datos personales que esa ley señale en relación con el cumplimiento de sus competencias de regulación y vigilancia para conseguir fines públicos. Asimismo, indicará en qué casos procede esa revisión.

No producirán efectos legales, la correspondencia que fuere sustraída ni la información obtenida como resultado de la intervención ilegal de cualquier comunicación".

Ver en: http://www.asamblea.go.cr/Centro_de_informacion/Consultas_SIL/SitePages/ConsultaProyectos.aspx consulta realizada el 16 de julio de 2020.

[386] El señalado capítulo sexto se inicia en el artículo 92, que precisamente se refiere a la tutela judicial, al señalar: "El Estado garantiza, de conformidad con la ley, que las personas puedan acceder a los órganos judiciales a fin de obtener una tutela efectiva de sus derechos e intereses legítimos. Las decisiones judiciales son de obligatorio cumplimiento y su irrespeto deriva responsabilidad para quien las incumpla".

> *modificación, actualización o cancelación. El uso y tratamiento de estos datos se realiza de conformidad con lo establecido en la ley"*.

Disposición que además reconoce la existencia de los derechos vinculados a la protección de datos de carácter personal como son los de corrección, rectificación, modificación, actualización o cancelación. Esta disposición de la Carta Política hay que entenderla en armonía con el artículo 48, que si está contenido en el Capítulo II sobre los "Derechos" que a su turno señala:

> *"Todas las personas tienen derecho a que se les respete su intimidad personal y familiar, su propia imagen y voz, su honor e identidad personal"*.

Ecuador

La regulación constitucional de la protección de datos en Ecuador se encuentra en el Capítulo Sexto, que se titula "Derechos de Libertad" específicamente en el numeral diecinueve del artículo 66, que dispone:

> *"Se reconoce y garantiza a las personas (…) 19. El derecho a la protección de datos de carácter personal, que incluye el acceso y la decisión sobre información y datos de este carácter, así como su correspondiente protección. La recolección, archivo, procesamiento, distribución o difusión de estos datos o información requerirán la autorización del titular o el mandato de la ley"*.

A su vez el artículo 92 de la Constitución del Ecuador, reconoce el hábeas data, al señalar:

> *"Toda persona, por sus propios derechos o como representante legitimado para el efecto, tendrá derecho a conocer de la existencia y a acceder a los documentos, datos genéticos, bancos o archivos de datos personales e informes que sobre sí misma, o sobre sus bienes, consten en entidades públicas o privadas, en soporte material o electrónico. Asimismo, tendrá derecho a conocer el uso que se haga de ellos, su finalidad, el origen y destino de información personal y el tiempo de vigencia del archivo o banco de datos. Las personas responsables de los bancos o archivos de datos personales podrán difundir la información archivada con autorización de su titular o de la ley. La persona titular de los datos podrá solicitar al responsable el acceso sin costo al archivo, así como la actualización de los datos, su rectificación, eliminación o anulación. En el caso de datos sensibles, cuyo archivo deberá estar autorizado por la ley o por la persona titular, se exigirá la adopción de las medidas de seguridad necesarias. Si no se atendiera su solicitud, ésta podrá acudir a la jueza o juez. La persona afectada podrá demandar por los perjuicios ocasionados"*.

El Salvador

En El Salvador, la Constitución de la República no reconoce explícitamente el derecho al acceso, control y protección de nuestros datos personales o mejor conocido como derecho a la autodeterminación informativa, sin embargo, este se deriva de lo establecido en su artículo 2, el cual sirvió de base para que la Sala de lo Constitucional reconociera la preservación de la información de las personas que se encuentra contenida en registros públicos o privados frente a la utilización arbitraria.

Dispone el artículo 2 de la Constitución de El Salvador:

> *"Toda persona tiene derecho a la vida, a la integridad física y moral, a la libertad, a la seguridad, al trabajo, a la propiedad y posesión, y a ser protegida en la conservación y defensa de los mismos. Se garantiza el derecho al honor, a la intimidad personal y familiar y a la propia imagen.*
> *Se establece la indemnización, conforme a la ley, por daños de carácter moral".*

Guatemala

En Guatemala, el artículo 31 de su Constitución, relativo al Acceso a archivos y registros estatales, dispone que:

> *"Toda persona tiene el derecho de conocer lo que de ella conste en archivos, fichas o cualquier otra forma de registros estatales, y la finalidad a que se dedica esta información, así como a corrección, rectificación y actualización. Quedan prohibidos los registros y archivos de filiación política, excepto los propios de las autoridades electorales y de los partidos políticos".*

Por consiguiente, este derecho no considera el derecho a conocer datos o información de sus titulares contenida en registros, archivos o fichas de entidades privadas o de organismos no estatales.

Honduras

En el caso hondureño, su Constitución aborda la protección de datos de carácter personal en diversas disposiciones. En efecto, garantiza el derecho a la intimidad personal y la inviolabilidad de las comunicaciones incorporando a su lista de recursos el hábeas data en el año 2015, específicamente en el artículo 182 N° 2. Sin embargo, el conocimiento de este recurso se enfoca exclusivamente a la Sala de lo Constitucional de la Corte Suprema de Justicia lo que limita el acceso a la población general para la interposición de este recurso, ya que la Corte Suprema solamente tiene sede en la ciudad capital y este recurso debe ser interpuesto directamente por la persona cuya información es la que consta en los registros.

Los siguientes artículos de la Constitución Hondureña determinan cómo se encuentran regulados diferentes derechos relacionados con la protección de datos de carácter personal:

Artículo 76:

> *"Se garantiza el derecho al honor, a la intimidad personal, familiar y a la propia imagen".*

Artículo 100:

> *"Toda persona tiene derecho a la inviolabilidad y al secreto de las comunicaciones, en especial de las postales, telegráficas y telefónicas, salvo resolución judicial. Los libros y comprobantes de los comerciantes y los documentos personales únicamente estarán sujetos a inspección o fiscalización de la autoridad competente, de conformidad con la Ley. Las comunicaciones, los libros, comprobantes y documentos a que se refiere el presente artículo, que fueren violados o sustraídos, no harán fe en juicio. En todo caso, se guardará siempre el secreto respecto de los asuntos estrictamente privados que no tengan relación con el asunto objeto de la acción de la autoridad."*
> *El Estado reconoce la garantía de Hábeas Corpus o de exhibición Personal, y de hábeas data. En consecuencia, en el Hábeas Corpus o exhibición Personal, toda*

persona agraviada o cualquiera otra en nombre de esta tiene derecho a promoverla, en el Hábeas Data en cambio, únicamente puede promoverla la persona cuyos datos personales o familiares consten en los archivos, registros públicos o privados regulados en el Artículo 182 N°2 de la Constitución, el cual dispone: "Toda persona tiene el derecho de acceso a la información sobre si misma o sus bienes en forma expedita y no onerosa, ya esté contenida en bases de datos, registros públicos o privados y, en el caso de que fuere necesario, actualizarla, rectificarla y/o suprimirla. No podrá afectarse el secreto de las fuentes de información periodística. Las acciones de Hábeas Corpus o de Hábeas Data se deben ejercer sin necesidad de poder ni de formalidad alguna, verbalmente o por escrito, utilizando cualquier medio de comunicación, en horas o días hábiles e inhábiles y libres de costas. Únicamente deben conocer de la garantía de Hábeas Data la Sala de lo Constitucional de la Corte Suprema de Justicia, quien tiene la obligación ineludible de proceder de inmediato para hacer cesar cualquier violación a los derechos del honor, intimidad personal o familiar y a la propia imagen. Los titulares de los órganos jurisdiccionales no pueden desechar la acción de Hábeas Corpus o Exhibición personal e igualmente tienen la obligación ineludible de proceder de inmediato para hacer cesar la violación de la libertad y la seguridad personal. En ambos casos, los titulares de los órganos jurisdiccionales que dejen de admitir estas acciones constitucionales incurren en responsabilidad penal y administrativa. Las autoridades que ordenaren y los agentes que ejecutaren el ocultamiento del detenido o que en cualquier forma quebranten esta garantía incurren en el delito de detención ilegal".

México

México, que es uno de los países de la región que más desarrollo en el ámbito legislativo tiene en materia de protección de datos de carácter personal, reconoce este derecho en el inciso segundo del artículo 16 de la Constitución, al señalar que:

"Toda persona tiene derecho a la protección de sus datos personales, al acceso, rectificación y cancelación de los mismos, así como a manifestar su oposición, en los términos que fije la ley, la cual establecerá los supuestos de excepción a los principios que rijan el tratamiento de datos, por razones de seguridad nacional, disposiciones de orden público, seguridad y salud públicas o para proteger los derechos de terceros".

Como se puede apreciar los Estados Unidos Mexicanos reconocen expresamente el derecho a la protección de datos personales, así como las causales de excepción que habilitan el tratamiento de datos de carácter personal.

Nicaragua

Por su parte Nicaragua, en la Constitución Política, reconoce en su artículo 26 el derecho a la protección y respeto a la vida privada, estableciendo que:

"Toda persona tiene derecho: 1) A su vida privada y a la de su familia. 2) Al respeto de su honra y reputación. 3) A conocer toda información que sobre ella se haya registrado en las entidades de naturaleza privada y pública, así como el derecho de saber por qué y con qué finalidad se tiene esa información. 4) A la inviolabilidad de su domicilio, su

> *correspondencia y sus comunicaciones de todo tipo. El domicilio sólo puede ser allanado por orden escrita de juez competente, excepto: 1. Si los que habitaren en una casa manifestaren que allí se está cometiendo un delito o de ella se pidiera auxilio; 2. si por incendio, inundación u otra causa semejante, se hallare amenazada la vida de los habitantes o de la propiedad; 3. cuando se denunciare que personas extrañas han sido vistas en una morada, con indicios manifiestos de ir a cometer un delito; 4. en caso de persecución actual e inmediata de un delincuente; 5. para rescatar a la persona que sufra secuestro.*
> *En todos los casos se procederá de acuerdo con la Ley. La Ley fija los casos y procedimientos para el examen de documentos privados, libros contables y sus anexos, cuando sea indispensable para esclarecer asuntos sometidos al conocimiento de los Tribunales de Justicia o por motivos fiscales. Las cartas, documentos y demás papeles privados sustraídos ilegalmente no producen efecto alguno en juicio o fuera de él."*

Igualmente, la Carta Magna nicaragüense, reconoce el derecho de amparo en su artículo 45, al señalar: "Las personas cuyos derechos constitucionales hayan sido violados o estén en peligro de serlo, pueden interponer el Recurso de Exhibición Personal o de Amparo, según el caso y de acuerdo con la Ley de Amparo."

En este sentido, en el año 2013, la Asamblea Nacional aprobó la reforma de la Ley de Amparo, agregándose el recurso de habeas data. Mediante esta reforma los ciudadanos pueden recurrir ante la Sala Constitucional de la Corte Suprema de Justicia cuando crean que su derecho a la privacidad y al correcto uso de sus datos personales haya sido vulnerado. Este recurso puede ser interpuesto ante la Sala Constitucional de la Corte Suprema de Justicia treinta días después de haber agotado la vía administrativa, debiendo emitir respuesta la Sala en el plazo de sesenta días. Igualmente, se habilita a las personas a exigir la oposición, modificación, supresión, bloqueo, inclusión y rectificación de los datos personales.

Panamá

En Panamá, con la última reforma constitucional el año 2004, se reconoció la importancia del derecho a la autodeterminación informativa o libertad informática al otorgarle a este derecho rango constitucional e incluirlo, aunque no explícitamente, en el Título III correspondiente a los Derechos Fundamentales, Capítulo I sobre Garantías Fundamentales. Dispone la Constitución en su artículo 29:

> *"La correspondencia y demás documentos privados son inviolables y no pueden ser examinados ni retenidos, si no por mandato de autoridad competente y para fines específicos, de acuerdo con las formalidades legales. En todo caso, se guardará absoluta reserva sobre los asuntos ajenos al objeto del examen o de la retención.*
> *El registro de cartas y demás documentos o papeles se practicará siempre en presencia del interesado o en presencia de una persona de su familia, o, en su defecto, de dos vecinos honorables del mismo lugar.*
> *Todas las comunicaciones privadas son inviolables y no podrán ser interceptadas o grabadas, si no por mandato de autoridad judicial.*
> *El incumplimiento de esta disposición impedirá la utilización de sus resultados con pruebas, sin perjuicio de las responsabilidades penales en que puedan incurrir sus autores".*

Paraguay

Por su parte, la Constitución Paraguaya en materia de protección de datos personales toma como referencia el artículo 33 referido al derecho a la intimidad, el cual señala;

> *"La intimidad personal y familiar, así como el respeto a la vida privada, son inviolables. La conducta de las personas, en tanto no afecte el orden público establecido en la ley o a los derechos de terceros, estará exenta de la autoridad pública.*
> *Se garantiza el derecho a la protección de la intimidad, de la dignidad y de la imagen privada de la persona".*

También el artículo 135 de la Constitución de Paraguay, contenido en el Capítulo XII sobre las garantías constitucionales, establece el habeas data, al señalar:

> *"Toda persona podrá acceder a la información y a los datos que sobre sí misma, o sobre sus bienes, obren en registros oficiales o privados de carácter público, así como conocer el uso que se haga de los mismos y su finalidad. Podrá solicitar ante el magistrado competente la actualización, la rectificación o la destrucción de aquellos, si fuesen erróneos o afectaran ilegítimamente sus derechos".*

Perú

Si bien Perú no regula expresamente la protección de datos personales, esta se desprende del artículo 2 referido a los derechos fundamentales, el 2.5 en su primera parte dispone que toda persona tiene derecho:

> *"A solicitar sin expresión de causa la información que requiera y a recibirla de cualquier entidad pública, en el plazo legal, con el costo que suponga el pedido. Se exceptúan las informaciones que afectan la intimidad personal y las que expresamente se excluyan por ley o por razones de seguridad nacional".*

Y luego el 2.6 señala que toda persona tiene derecho:

> *"A que los servicios informáticos, computarizados o no, públicos o privados, no suministren informaciones que afecten la intimidad personal y familiar".*

De igual forma la Constitución peruana reconoce el hábeas data en el numeral 3 del artículo 200, al disponer:

> *"La Acción de Hábeas Data, que procede contra el hecho u omisión, por parte de cualquier autoridad, funcionario o persona, que vulnera o amenaza los derechos a que se refiere el artículo 2, incisos 5 y 6 de la Constitución".*

República Dominicana

Por su parte, República Dominicana en el artículo 44 de su Constitución, aborda el derecho a la intimidad y el honor personal, señalando que:

> *"Toda persona tiene derecho a la intimidad. Se garantiza el respeto y la no injerencia en la vida privada, familiar, el domicilio y la correspondencia del individuo. Se reconoce el derecho al honor, al buen nombre y a la propia imagen. Toda autoridad o particular que los viole está obligado a resarcirlos o repararlos conforme a la ley. Por tanto: 2) Toda persona tiene el derecho a acceder a la información y a los datos que*

> *sobre ella o sus bienes reposen en los registros oficiales o privados, así como conocer el destino y el uso que se haga de los mismos, con las limitaciones fijadas por la ley. El tratamiento de los datos e informaciones personales o sus bienes deberá hacerse respetando los principios de calidad, licitud, lealtad, seguridad y finalidad. Podrá solicitar ante la autoridad judicial competente la actualización, oposición al tratamiento, rectificación o destrucción de aquellas informaciones que afecten ilegítimamente sus derechos".*

Del mismo modo el artículo 70 de la Carta Política dispone:

> "*Hábeas data. Toda persona tiene derecho a una acción judicial para conocer de la existencia y acceder a los datos que de ella consten en registros o bancos de datos públicos o privados y, en caso de falsedad o discriminación, exigir la suspensión, rectificación, actualización y confidencialidad de aquéllos, conforme a la ley. No podrá afectarse el secreto de las fuentes de información periodística".*

Uruguay

Uruguay no reconoce explícitamente el derecho a la protección de datos, por cuanto este se deriva de una norma constitucional genérica, como es el artículo 72 de su Carta Política, el cual dispone que:

> *"La enumeración de derechos, deberes y garantías hecha por la Constitución, no excluye los otros que son inherentes a la personalidad humana o se derivan de la forma republicana de gobierno".*

Sin embrago, dicho país ha tenido un importante desarrollo de la protección de datos a nivel legislativo, en efecto, en el año 2008 se aprobó la Ley N° 18.331 de 11 de agosto de ese año, que regula la protección de datos personales y la acción de habeas data, la cual fue posteriormente reglamentada por el decreto N° 414/009.

El artículo 1° de la señalada Ley, expresa que la protección de datos personales es un derecho humano y se encuentra comprendido dentro del artículo constitucional mencionado anteriormente. La Ley crea en el artículo 31 el órgano de control encargado de vigilar el cumplimiento de la normativa en la materia, denominado Unidad Reguladora y de Control de Datos Personales. Dicha Unidad está dotada de amplia autonomía técnica con competencia en todo el país. Se crea como un órgano desconcentrado de la Agencia para el Desarrollo del Gobierno de Gestión Electrónica y Sociedad de la Información y del Conocimiento, AGESIC. La Unidad está dirigida por un Consejo integrado por tres miembros, uno de ellos es el Director Ejecutivo de AGESIC, y dos designados por el Poder Ejecutivo.

Venezuela

Por último, en Venezuela, la Constitución de la República Bolivariana, señala en su artículo 60, que:

> "*Toda persona tiene derecho a la protección de su honor, vida privada, intimidad, propia imagen, confidencialidad, y reputación. La Ley limitará el uso de información para garantizar el honor, y la intimidad personal y familiar de los ciudadanos".*

A esto se suma el artículo 28 de la Carta Magna, el cual señala que; Toda persona tiene el derecho de acceder a la información y a los datos que sobre sí misma o sobre sus bienes consten en registros oficiales o privados, con las excepciones que establezca la ley, así como de conocer el uso que se haga de los mismos y su finalidad, y de solicitar ante el tribunal competente la actualización, la rectificación o la destrucción de aquellos, si fuesen erróneos o afectasen ilegítimamente sus derechos. Igualmente, podrá acceder a documentos de cualquier naturaleza que contengan información cuyo conocimiento sea de interés para comunidades o grupos de personas. Queda a salvo el secreto de las fuentes de información periodística y de otras profesiones que determine la ley[387].

Algunas consideraciones sobre el tratamiento constitucional de la Protección de Datos en Latinoamérica

Como se puede observar, la regulación de la protección de datos personales en las constituciones latinoamericanas es diversa, y en muchos casos más bien deriva de una interpretación o extensión de los derechos a la intimidad, vida privada, honra o imagen que de una mención explícita que lo reconozca. En otros casos, más que una referencia o regulación a la protección de datos las Cartas Políticas se refieren al habeas data, como un mecanismo o acción para tutelar el derecho a la protección de datos, aun cuando este no tenga un tratamiento expreso.

En otras constituciones no hay referencia explícita alguna ni a la protección de datos, ni al habeas data, no obstante, su regulación queda radicada al ámbito legislativo. En el siguiente cuadro se expondrá cómo la normativa latinoamericana aborda esta materia en sus respectivas constituciones, reiterando que, en muchos casos, por ejemplo, la regulación del habeas data, como en el caso chileno, no está en la constitución si no que es regulada por el legislador:

Cuadro N° 1:

Constitución	**Referencia expresa al derecho de protección de datos**	**Referencia implícita al derecho de protección de datos**	**Habeas Data**
Argentina	No	Sí	Sí
Bolivia	No	Sí	Sí
Brasil	No	Sí	Sí
Chile	Sí	-	No
Colombia	No	Sí	No

[387]Asimismo, la Ley Orgánica del Tribunal Supremo de Justicia, (TSJ), también precisa en su artículo 167 que los ciudadanos tienen derecho a conocer la información que sobre ellos se refiera y esté contenida en los archivos de los bancos públicos y privados, además podrá solicitar la confidencialidad.

Costa Rica	No	Sí	No
Cuba	Sí	-	No
Ecuador	Sí	-	Sí
El Salvador	No	Sí	No
Guatemala	No	Sí	No
Honduras	No	Sí	Sí
México	Sí	-	No
Nicaragua	No	Sí	Sí
Panamá	No	Sí	No
Paraguay	No	Sí	Sí
Perú	No	Sí	Sí
República Dominicana	Sí	-	Sí
Uruguay	No	Sí	No
Venezuela	Sí	-	Sí

Fuente: elaboración propia.

La protección de Datos en las Legislaciones Latinoamericanas

Habiendo revisado la regulación a nivel constitucional de la protección de datos en los países latinoamericanos, corresponde ahora revisar de qué manera las legislaciones de la región abordan la materia.

Argentina

En primer lugar, hay que destacar la decisión de la Comisión de la Unión Europea singularizada como C 1731, de fecha 30 de junio de 2003, que le dio a la República Argentina el carácter de país adecuado en materia de protección de datos personales, decisión que se sustentó fundamentalmente en la legislación de ese país que regula hasta el día de hoy esta materia.

En efecto, el 2 de noviembre del año 2000 se publica la Ley N°25.326[388] sobre protección de los datos personales, la que consta de siete capítulos; el capítulo primero aborda las Disposiciones generales, en las que se establece el objeto de la ley (artículo 1°)[389] y las

[388] Ver en: http://servicios.infoleg.gob.ar/infolegInternet/anexos/60000-64999/64790/texact.htm

[389] Artículo 1°: "La presente ley tiene por objeto la protección integral de los datos personales asentados en archivos, registros, bancos de datos, u otros medios técnicos de tratamiento de datos, sean estos públicos, o privados destinados a dar informes, para garantizar el derecho al honor y a la intimidad de las personas, así como también el acceso a la información que sobre las mismas se registre, de conformidad a lo establecido en el artículo 43, párrafo tercero de la Constitución Nacional".

definiciones de los términos que esa ley utiliza, tales como: datos personales, datos sensibles, archivo, registro o base o banco de datos, tratamiento de datos, responsable de archivo, registro o base o banco de datos, datos informatizados, titular de datos, usuario de datos y disociación de datos (artículo 2°).

El capítulo segundo se refiere a los Principios generales relativos a la protección de datos entre los artículos 3 y 12. En el artículo 3 se aborda la licitud de los datos y el principio de finalidad de las bases o archivos de datos[390], en el artículo 4 se hace referencia a la calidad de los datos, en el artículo 5 se regula el consentimiento del titular para el tratamiento de datos de carácter personal, disponiendo que el tratamiento de datos personales es ilícito cuando el titular no hubiere prestado su consentimiento libre, expreso e informado, el que deberá constar por escrito, o por otro medio que permita se le equipare, de acuerdo a las circunstancias y que el consentimiento prestado con otras declaraciones, deberá figurar en forma expresa y destacada, previa notificación al requerido de datos, de la información descrita en el artículo 6° de la ley. También este artículo aborda aquellos casos en que el consentimiento no es necesario para el tratamiento de datos[391]; en el artículo 6 inciso final además se reconocen los derechos de acceso, rectificación y supresión de datos, en el artículo 7 se hace referencia a la categoría de datos sensibles y su tratamiento, en el artículo 8 se abordan los datos de salud señalando que "Los establecimientos sanitarios públicos o privados y los profesionales vinculados a las ciencias de la salud pueden recolectar y tratar los datos personales relativos a la salud física o mental de los pacientes que acudan a los mismos o que estén o hubieren estado bajo tratamiento de aquellos, respetando los principios del secreto profesional". El artículo 9[392] se refiere a la seguridad de los datos, en el artículo 10 se regula el deber de confidencialidad, y el artículo 11 trata la cesión de los datos. Finalmente, el artículo 12 regula la transferencia internacional de datos[393].

---

[390] "La formación de archivos de datos será lícita cuando se encuentren debidamente inscriptos, observando en su operación los principios que establece la presente ley y las reglamentaciones que se dicten en su consecuencia. Los archivos de datos no pueden tener finalidades contrarias a las leyes o a la moral pública".

[391] "No será necesario el consentimiento cuando: a) Los datos se obtengan de fuentes de acceso público irrestricto; b) Se recaben para el ejercicio de funciones propias de los poderes del Estado o en virtud de una obligación legal; c) Se trate de listados cuyos datos se limiten a nombre, documento nacional de identidad, identificación tributaria o previsional, ocupación, fecha de nacimiento y domicilio; d) Deriven de una relación contractual, científica o profesional del titular de los datos, y resulten necesarios para su desarrollo o cumplimiento; e) Se trate de las operaciones que realicen las entidades financieras y de las informaciones que reciban de sus clientes conforme las disposiciones del artículo 39 de la Ley 21.526".

[392] "1. El responsable o usuario del archivo de datos debe adoptar las medidas técnicas y organizativas que resulten necesarias para garantizar la seguridad y confidencialidad de los datos personales, de modo de evitar su adulteración, pérdida, consulta o tratamiento no autorizado, y que permitan detectar desviaciones, intencionales o no, de información, ya sea que los riesgos provengan de la acción humana o del medio técnico utilizado. 2. Queda prohibido registrar datos personales en archivos, registros o bancos que no reúnan condiciones técnicas de integridad y seguridad".

[393] "1. Es prohibida la transferencia de datos personales de cualquier tipo con países u organismos internacionales o supranacionales, que no proporcionen niveles de protección adecuados. 2. La prohibición no regirá en los siguientes supuestos: a) Colaboración judicial internacional; b) Intercambio de datos de carácter médico, cuando así lo exija el tratamiento del afectado, o una investigación epidemiológica, en tanto se realice en los términos del inciso e) del artículo anterior; c) Transferencias bancarias o bursátiles, en lo relativo a las transacciones respectivas y conforme la legislación que les resulte aplicable; d) Cuando la transferencia se hubiera acordado en el marco de tratados internacionales en los cuales la República Argentina sea parte; e) Cuando la transferencia

El Capítulo tercero trata los derechos de los titulares de datos, regulando el derecho de información en el artículo 13, el derecho de acceso en el artículo 14, el derecho de rectificación, actualización o supresión en el artículo 16, así como la gratuidad en el ejercicio de tales derechos en el artículo 19. El Capítulo cuarto aborda a los usuarios y responsables de archivos, registros, y bancos de datos, entre los artículos 21 al 28.

El Capítulo quinto hace referencia al control y a la autoridad encargada de su ejercicio, el artículo 29 regula las funciones y atribuciones de la autoridad de control, así como las características de la configuración de dicha entidad, cual es la autonomía funcional y la descentralización del mismo como órgano dependiente del Ministerio de Justicia y Derechos Humanos, mayores detalles de la autoridad de control así como su configuración y atribuciones serán abordadas en el siguiente capítulo de este trabajo. El Capítulo sexto se refiere a las sanciones, abordando el artículo 31 las sanciones administrativas y el artículo 32 las sanciones penales.

Por último, el Capítulo séptimo aborda la Acción de protección de datos personales o habeas data, distingüendo entre la procedencia de la misma (artículo 33)[394], la legitimación activa (artículo 34)[395] y pasiva (artículo 35)[396], la competencia (artículo 36)[397], el procedimiento aplicable (artículo 37)[398], los requisitos de la demanda (artículo 38)[399], su tramitación (artículo

---

tenga por objeto la cooperación internacional entre organismos de inteligencia para la lucha contra el crimen organizado, el terrorismo y el narcotráfico".

394 "1. La acción de protección de los datos personales o de hábeas data procederá: a) para tomar conocimiento de los datos personales almacenados en archivos, registros o bancos de datos públicos o privados destinados a proporcionar informes, y de la finalidad de aquéllos; b) en los casos en que se presuma la falsedad, inexactitud, desactualización de la información de que se trata, o el tratamiento de datos cuyo registro se encuentra prohibido en la presente ley, para exigir su rectificación, supresión, confidencialidad o actualización".

395 "La acción de protección de los datos personales o de hábeas data podrá ser ejercida por el afectado, sus tutores o curadores y los sucesores de las personas físicas, sean en línea directa o colateral hasta el segundo grado, por sí o por intermedio de apoderado. Cuando la acción sea ejercida por personas de existencia ideal, deberá ser interpuesta por sus representantes legales, o apoderados que éstas designen al efecto. En el proceso podrá intervenir en forma coadyuvante el Defensor del Pueblo".

396 "La acción procederá respecto de los responsables y usuarios de bancos de datos públicos, y de los privados destinados a proveer informes".

397 "Será competente para entender en esta acción el juez del domicilio del actor; el del domicilio del demandado; el del lugar en el que el hecho o acto se exteriorice o pudiera tener efecto, a elección del actor. Procederá la competencia federal: a) cuando se interponga en contra de archivos de datos públicos de organismos nacionales, y b) cuando los archivos de datos se encuentren interconectados en redes interjurisdicciones, nacionales o internacionales".

398 "La acción de hábeas data tramitará según las disposiciones de la presente ley y por el procedimiento que corresponde a la acción de amparo común y supletoriamente por las normas del Código Procesal Civil y Comercial de la Nación, en lo atinente al juicio sumarísimo".

399 "1. La demanda deberá interponerse por escrito, individualizando con la mayor precisión posible el nombre y domicilio del archivo, registro o banco de datos y, en su caso, el nombre del responsable o usuario del mismo. En el caso de los archivos, registros o bancos públicos, se procurará establecer el organismo estatal del cual dependen. 2. El accionante deberá alegar las razones por las cuales entiende que en el archivo, registro o banco de datos individualizado obra información referida a su persona; los motivos por los cuales considera que la información que le atañe resulta discriminatoria, falsa o inexacta y justificar que se han cumplido los recaudos que hacen al ejercicio de los derechos que le reconoce la presente ley. 3. El afectado podrá solicitar que mientras dure el procedimiento, el registro o banco de datos asiente que la información cuestionada está sometida a un proceso

39)[400] y los plazos y requisitos de la sentencia (artículo 43). Finalmente, el artículo 44[401] aborda el ámbito de aplicación de la ley.

Argentina en el año 2016, mediante la Ley N° 27.275[402] creó la Agencia de Acceso a la Información Pública a quien atribuyó conjuntamente las funciones de garantizar el acceso a la información pública y la protección de datos personales, entidad de la cual depende la Dirección Nacional de Protección de Datos Personales.

El 19 de septiembre del año 2018, se presentó un proyecto de ley que buscaba actualizar la vigente legislación en materia de protección de datos en Argentina, proyecto que no ha tenido avances en su tramitación[403]. Más recientemente, el 2 de enero del año 2019, se publica la Ley 27.483, que aprueba el Convenio para la Protección de las Personas con respecto al Tratamiento Automatizado de Datos de Carácter Personal, más conocido como Convenio 108 de Europa, suscrito en la ciudad de Estrasburgo, República Francesa, el día 28 de enero de 1981, y el Protocolo Adicional al Convenio para la Protección de las personas con respecto al Tratamiento Automatizado de Datos de Carácter Personal, a las autoridades de control y a los flujos transfronterizos de datos, suscrito el día 8 de noviembre de 2001[404].

Brasil

En agosto de 2018 se aprueba la Ley General de Protección de Datos Personales N° 13.709[405], que entraría en vigor en agosto de 2020, ya que estableció una vacancia legal de 24 meses, plazo que nuevamente ha sido postergado parcialmente hasta el 3 de mayo de 2021, mediante la Medida Provisional N° 959/2020, publicada en el Diario Oficial de la Unión el 29 de abril[406].

---

judicial. 4. El Juez podrá disponer el bloqueo provisional del archivo en lo referente al dato personal motivo del juicio cuando sea manifiesto el carácter discriminatorio, falso o inexacto de la información de que se trate. 5. A los efectos de requerir información al archivo, registro o banco de datos involucrado, el criterio judicial de apreciación de las circunstancias requeridas en los puntos 1 y 2 debe ser amplio".

[400] "1. Admitida la acción el juez requerirá al archivo, registro o banco de datos la remisión de la información concerniente al accionante. Podrá asimismo solicitar informes sobre el soporte técnico de datos, documentación de base relativa a la recolección y cualquier otro aspecto que resulte conducente a la resolución de la causa que estime procedente. 2. El plazo para contestar el informe no podrá ser mayor de cinco días hábiles, el que podrá ser ampliado prudencialmente por el juez".

[401] "Las normas de la presente ley contenidas en los Capítulos I, II, III y IV, y artículo 32 son de orden público y de aplicación en lo pertinente en todo el territorio nacional. Se invita a las provincias a adherir a las normas de esta ley que fueren de aplicación exclusiva en jurisdicción nacional. La jurisdicción federal regirá respecto de los registros, archivos, bases o bancos de datos interconectados en redes de alcance interjurisdiccional, nacional o internacional".

[402]Ver en: http://servicios.infoleg.gob.ar/infolegInternet/anexos/265000-269999/265949/texact.htm consulta realizada el 24 de julio de 2020.

[403] Ver en: https://www.argentina.gob.ar/sites/default/files/mensaje_ndeg_147-2018_datos_personales.pdf consulta realizada el 21 de julio de 2020.

[404] Ver en: https://www.boletinoficial.gob.ar/detalleAviso/primera/199254/20190102 consulta realizada el 21 de julio de 2020.

[405] Ver en: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709compilado.htm consulta realizada el 22 de julio de 2020.

[406] Ver en: http://www.in.gov.br/web/dou/-/medida-provisoria-n-959-de-29-de-abril-de-2020-254499639 consulta realizada el 22 de julio de 2020.

Es una postergación parcial por cuanto se mantiene la entrada en vigor para agosto del año 2020 para algunos de sus articulados, como por ejemplo el artículo 55 que regula la creación de la Autoridad Nacional para la Protección de Datos Personales -ANPD, según lo previsto en el artículo 65[407] de la mencionada ley, no pudiendo eso sí, esta entidad aplicar sanción alguna hasta el 3 de mayo de 2021.

La Ley 13.709, es la primera norma legislativa que regula sistémicamente la protección de datos en Brasil, que está fuertemente influenciada por el RGPD de la UE. Antes de ella, la regulación de la protección de datos brasilera se encontraba dispersa en diversas leyes, como por ejemplo, en la Ley N° 10.406/2002, en la que se contiene el Código Civil que a propósito de los atributos de la personalidad establece la inviolabilidad de la vida privada. En la Ley N°12.965/2014 sobre el Marco Civil de Internet, que regula los principios, garantías, derechos y deberes del uso de internet, como también aborda la recogida, tratamiento y almacenamiento de datos personales a través de internet, o en la Ley N° 8.078/2009 que contiene el Código de Defensa del Consumidor, y establece el derecho de los consumidores a acceder a su información registrada en archivos y bases de datos sobre su consumo.

La ley de protección de datos brasileña contiene 65 artículos que se distribuyen en diez capítulos. El Capítulo I se titula Disposiciones Preliminares, el Capítulo II Del Tratamiento de Datos Personales, el Capítulo III se titula De los Derechos del Titular, el Capítulo IV Del Tratamiento de Datos Personales por el Público, el Capítulo V se refiere a la Transferencia Internacional de Datos, el Capítulo VI se refiere a los Agentes de Tratamiento de Datos Personales, el Capítulo VII se titula Seguridad y Buenas Prácticas, el Capítulo VIII se refiere a la Inspección, el Capítulo IX se titula De la Autoridad Nacional de Protección de Datos (ANPD) y El Consejo Nacional de Protección de Datos Personales y Privacidad, finalmente el Capitulo X se refiere a las Disposiciones Finales y Transitorias.

El artículo 1° de esta ley señala que su propósito es regular el tratamiento de datos personales incluso en medios digitales, delimitando además su objetivo, cual es proteger los derechos fundamentales de libertad y privacidad y el libre desarrollo de la personalidad de la persona natural.

El artículo segundo de la ley, establece las directrices normativas sobre las que se sustenta la protección de datos en Brasil, y que es el respeto por la privacidad; la autodeterminación informativa; libertad de expresión, información, comunicación y opinión; la inviolabilidad de la intimidad, el honor y la imagen; el desarrollo e innovación económica y tecnológica; la libre empresa, libre competencia y protección del consumidor; y los derechos humanos, el libre desarrollo de la personalidad, la dignidad y el ejercicio de la ciudadanía por parte de las personas físicas.

La aplicación de la ley incluye a todas las instituciones brasileñas que manejan datos personales en sus operaciones u ofrecen sus productos y servicios, tanto del sector público

[407] Esta Ley entra en vigor: I - 28 de diciembre de 2018, en relación con los arts. 55-A, 55-B, 55-C, 55-D, 55-E, 55-F, 55-G, 55-H, 55-I, 55-J, 55-K, 55-L, 58- A y 58-B; y IA - 1 de agosto de 2021, en relación con los arts. 52, 53 y 54; II - el 3 de mayo de 2021, con respecto a los otros artículos, esta nueva prórroga se establece por la Medida Provisional N° 959, de 2020.

como del privado. Propone además su aplicación para entidades extranjeras con sede en Brasil, que practican actividades de recolección de datos.

Así se desprende entre otras disposiciones de su artículo 3, que señala:

> *"Esta Ley se aplica a cualquier operación de procesamiento realizada por una persona física o jurídica de derecho público o privado, independientemente del medio, el país de su sede o el país donde se encuentran los datos, siempre que: I - la operación de tratamiento se lleva a cabo en el territorio nacional; II - la actividad de tratamiento tiene como objetivo ofrecer o suministrar bienes o servicios o procesar datos de personas ubicadas en el territorio nacional; o III - los datos personales sujetos al tratamiento se han recopilado en el territorio nacional.*
> *§ 1 Los datos personales cuyo titular se encuentra en el momento de la recopilación se consideran recopilados en el territorio nacional.*
> *Párrafo 2. Excepto por lo dispuesto en el ítem I de este artículo, el procesamiento de datos previsto en el ítem IV de la sección de art. 4to de esta Ley".*

Se exceptúan según se desprende del artículo 4 de la ley entre otros, lo datos personales tratados con fines académicos, artísticos o periodísticos, así como aquellos que involucren seguridad pública, defensa nacional, protección de la vida y políticas gubernamentales. Estos casos deben ser tratados por leyes específicas.

> *Artículo 4; "Esta Ley no se aplica al procesamiento de datos personales: I - realizado por una persona física con fines exclusivamente privados y no económicos; II - realizado con fines exclusivos: a) periodística y artística; o b) académicos, aplicando artes. 7 y 11 de esta Ley; III - realizado con fines exclusivos de: a) seguridad pública; b) defensa nacional; c) seguridad del Estado; o d) investigación y enjuiciamiento de delitos penales; o IV - provenientes de fuera del territorio nacional y que no son objeto de comunicación, uso compartido de datos con agentes de procesamiento brasileños u objeto de transferencia internacional de datos con un país que no sea el país de origen, siempre que el país de origen proporcione un grado de protección de datos personales adecuados a lo dispuesto en esta Ley.*
> *1. El tratamiento de los datos personales previsto en el punto III se regirá por una legislación específica, que establecerá medidas proporcionales y estrictamente necesarias para servir al interés público, observando el debido proceso legal, los principios generales de protección y los derechos del titular previstos en esta Ley.*
> *2. Se prohíbe el tratamiento de los datos a los que se hace referencia en el punto III del contenido de este artículo por una persona de derecho privado, excepto en los procedimientos bajo la tutela de una persona jurídica de derecho público, que serán objeto de un informe específico a la autoridad nacional y que deben cumplir con la limitación impuesta en el § 4 de este artículo.*
> *3. La autoridad nacional emitirá dictámenes técnicos o recomendaciones con respecto a las excepciones previstas en el punto III del contenido de este artículo y solicitará los informes responsables sobre el impacto en la protección de datos personales.*

El artículo 5 de la ley, al igual como ocurre con otras legislaciones en la materia, conceptualiza diversos términos, definiendo entre otros, el de datos personales de manera amplia como, "la información relacionada con una persona física identificada o identificable". También hay una categoría de datos sensibles, que distingue como "datos personales confidenciales", que son datos personales sobre el origen racial o étnico, convicción religiosa, opinión política,

afiliación sindical u organización de carácter religioso, filosófico o político, datos relacionados con la salud o la vida sexual, datos genéticos o biométricos, cuando están vinculados a una persona natural. Así como el tratamiento de datos y el consentimiento. El primero, dice la ley, es cualquier operación realizada con datos personales, como los referidos a la recopilación, producción, recepción, clasificación, uso, acceso, reproducción, transmisión, distribución, procesamiento, archivo, almacenamiento, eliminación, evaluación o control de información, modificación, comunicación, transferencia, difusión o extracción. Y sobre el consentimiento señala que este es la "expresión libre, informada y sin ambigüedades por la cual el titular está de acuerdo con el tratamiento de sus datos personales para un propósito específico". Es decir, si hay cambios de propósito o traspaso de datos a terceros, un nuevo consentimiento deberá ser solicitado. El usuario podrá, cuando desee, revocar su autorización, así como solicitar acceso, exclusión, portabilidad, complementación o corrección de los datos.

En caso de que el uso de la información lleve a una decisión automatizada indeseada, por ejemplo, el rechazo de financiamiento por parte de un banco, el usuario podrá solicitar una revisión humana del procedimiento. En general, la ley busca tutelar al ciudadano del uso abusivo e indiscriminado de sus datos. Además de pedir un consentimiento de manera clara y atender a las demandas del usuario sobre el mantenimiento o eliminación de los datos, las organizaciones y entidades solo podrán solicitar los datos que realmente sean necesarios para el fin propuesto. En ese sentido, el usuario podrá cuestionar si la exigencia de determinado dato tiene sentido o utilidad. Para ello, entre los artículos 17 y 22 de la ley se regulan los derechos de los titulares de los datos, distinguiendo entre el acceso e información respecto de los datos y su tratamiento; rectificación de datos incompletos, inexactos o desactualizados; remoción de datos almacenados o procesados; revocación del consentimiento; anonimización de datos innecesarios, excesivos o tratados de forma contraria a los dispuesto en la ley; portabilidad de datos y derecho a reclamación ante la autoridad nacional de protección de datos personales.

> *"Art. 17. Toda persona física tiene asegurado el título de sus datos personales y los derechos fundamentales de libertad, intimidad y privacidad están garantizados, de conformidad con los términos de esta Ley".*
>
> *Art. 18. El titular de los datos personales tiene derecho a obtener del controlador, en relación con los datos del titular tratado por él, en cualquier momento y previa solicitud: I - confirmación de la existencia de tratamiento; II - acceso a los datos; III - corrección de datos incompletos, inexactos u obsoletos; IV - anonimato, bloqueo o eliminación de datos innecesarios, excesivos o tratados que no cumplan con las disposiciones de esta Ley; V - portabilidad de datos a otro proveedor de servicios o productos, previa solicitud expresa, de conformidad con los reglamentos de la autoridad nacional, sujeto a secretos comerciales e industriales; VI - eliminación de datos personales tratados con el consentimiento del titular, excepto en los casos previstos en el art. 16 de esta Ley; VII - información de entidades públicas y privadas con las cuales el controlador hizo uso compartido de datos; VIII - información sobre la posibilidad de no dar consentimiento y sobre las consecuencias de la negativa; IX - revocación del consentimiento, de conformidad con el § 5 del art. 8 de esta Ley.*
> *1. El titular de los datos personales tiene derecho a presentar una petición en relación con sus datos contra el controlador ante la autoridad nacional.*

2. El titular puede oponerse al tratamiento realizado sobre la base de una de las hipótesis de renuncia al consentimiento, en caso de incumplimiento de las disposiciones de esta Ley.
3. Los derechos previstos en este artículo se ejercerán previa solicitud expresa del titular o representante legalmente constituido a un agente de procesamiento.
4. En caso de imposibilidad de adopción inmediata de la medida mencionada en el § 3 de este artículo, el controlador enviará al titular una respuesta en la que puede: I - comunico que no es un agente de procesamiento de datos e indique, siempre que sea posible, el agente; o II - indique las razones de hecho o de derecho que impiden la adopción inmediata de la medida.
Párrafo 5. La solicitud mencionada en el Párrafo 3 de este artículo será atendida sin costo alguno para el titular, dentro de los términos y en los términos previstos en el reglamento.
6. La persona responsable debe informar inmediatamente a los agentes de tratamiento con los que ha hecho uso compartido de los datos la corrección, eliminación, anonimización o bloqueo de los datos, para que repitan el mismo procedimiento, excepto en los casos en que esto la comunicación se demuestra imposible o implica un esfuerzo desproporcionado.
7. La portabilidad de los datos personales a los que se hace referencia en el ítem V de la sección de este artículo no incluye datos que ya hayan sido anonimizados por el controlador.
8. El derecho mencionado en el 1 de este artículo también se puede ejercer ante las agencias de protección al consumidor".
"Art. 19. Se proporcionará confirmación de existencia o acceso a datos personales, a solicitud del titular: I - en un formato simplificado, inmediatamente; o II - por medio de una declaración clara y completa, indicando el origen de los datos, la falta de registro, los criterios utilizados y el propósito del tratamiento, observando los secretos comerciales e industriales, proporcionados dentro de los 15 (quince) días contados a partir de la fecha de solicitud del titular.
1. Los datos personales se almacenarán en un formato que favorezca el ejercicio del derecho de acceso.
2. La información y los datos se pueden proporcionar, a discreción del titular: I - por medios electrónicos, seguros y adecuados para este propósito; o II - en forma impresa.
3. Cuando el tratamiento se origina en el consentimiento del titular o en un contrato, el titular puede solicitar una copia electrónica completa de sus datos personales, observando los secretos comerciales e industriales, bajo los términos de las regulaciones de la autoridad nacional, en un formato que permita su uso posterior., incluidas otras operaciones de tratamiento.
Párrafo 4. La autoridad nacional puede tener una disposición diferenciada sobre los plazos previstos en los puntos I y II del contenido de este artículo para sectores específicos".

"Art. 20. El interesado tiene derecho a solicitar la revisión de las decisiones tomadas únicamente sobre la base del procesamiento automatizado de datos personales que afectan sus intereses, incluidas las decisiones diseñadas para definir su perfil personal, profesional, de consumo y de crédito o aspectos de tu personalidad.

> *1. El controlador debe proporcionar, cuando se solicite, información clara y adecuada sobre los criterios y procedimientos utilizados para la decisión automatizada, observando los secretos comerciales e industriales.*
> *2º En caso de no ofrecer la información mencionada en el 1 de este artículo basada en la observancia del secreto comercial e industrial, la autoridad nacional puede llevar a cabo una auditoría para verificar aspectos discriminatorios en el procesamiento automatizado de datos personales".*
>
> *"Art. 21. Los datos personales relacionados con el ejercicio regular de los derechos por parte del titular no pueden utilizarse en detrimento suyo".*
>
> *"Art. 22. La defensa de los intereses y derechos de los interesados puede ejercerse en los tribunales, individual o colectivamente, de conformidad con las disposiciones de la legislación pertinente, en relación con los instrumentos de protección individual y colectiva".*

Sobre esta autoridad de control, que se abordará en mayor detalle en el siguiente capítulo de este trabajo de investigación, es importante señalar que esta ley crea una Autoridad de Control, la "Autoridad Nacional de Protección de Datos", vinculada al Ministerio de Justicia, que cuenta con autonomía técnica y cuya composición, funciones y responsabilidades se regulan entre los artículos 55-A y 55-L de la ley.

También mediante la Medida Provisoria N° 869 del 27 de diciembre de 2018, se crea el Consejo Nacional de Protección de Datos, contenido en el artículo 58-A de la ley, que tiene un carácter consultivo y cuya finalidad es asesorar y proponer acciones a la Autoridad Nacional de Protección de Datos.

El artículo 6 de la ley establece los principios generales para el tratamiento de datos personales, de manera similar al abordaje que sobre la materia hace el RGPD, distinguiendo entre los principios de finalidad, adecuación, necesidad, libre acceso, calidad de los datos, transparencia, seguridad, prevención, no discriminación, responsabilidad y rendición de cuentas.

A diferencia del RGPD en el que la protección del crédito es considerada como parte de la base legal del interés legítimo, en la ley de protección de datos brasilera la protección al crédito está expresamente prevista como base legal, con el fin de evitar dudas o contradicciones relacionadas con el tratamiento de datos personales para el análisis, formación y consulta del denominado "Catastro Positivo de Crédito"[408].

Respecto a la transferencia internacional de datos, el artículo 33 de la ley se refiere a los casos en que está permitida, siendo alguno de ellos que el país destinatario proporcione un grado de protección de datos equiparable a la ley brasilera, que exista un consentimiento especifico y por separado del titular de los datos para la realización de la transferencia internacional, que el controlador[409] garantice el cumplimiento de los principios, derechos del titular y el régimen de

[408] Regulado en la Ley n° 12.414/2011.

[409] Es el responsable de las decisiones sobre el tratamiento de datos, el cual debe designar un encargado, que actuará como vínculo entre este (el controlador), los titulares de los datos o interesados y la autoridad nacional de protección de datos. El encargado en la legislación brasilera es el equivalente al delegado de protección de datos

protección previsto en la ley o que la transferencia esté debidamente autorizada por la autoridad nacional de protección de datos.

Las sanciones por el incumplimiento a las disposiciones contenida en la ley se encuentran descritas entre los artículos 52 y 54, variando su intensidad dependiendo de la gravedad del incumplimiento. Si se comprueba la infracción, la entidad u organización responsable podrá recibir desde advertencias hasta una multa equivalente al 2% de su facturación. También podrán suspenderse total o parcialmente las actividades ligadas al tratamiento de datos, además de responder judicialmente a otras violaciones previstas por ley, cuando sea el caso.

El artículo 50 de la ley, establece los denominados códigos de conducta, que las empresas que gestionan bases de datos pueden adoptar, así como las asociaciones sectoriales que adhieran a códigos modelo que sean pre-autorizados por la autoridad nacional de protección de datos.

Chile

El 28 de agosto del año 1999 se pública en el Diario Oficial la Ley N° 19.628 sobre protección a la vida privada[410], siendo una de las primeras legislaciones latinoamericanas en abordar la protección de datos de carácter personales. Esta ley consta de 24 artículos permanentes y tres transitorios, cuya estructura se compone de un título preliminar, cinco títulos y un título final. El Título preliminar se refiere a las disposiciones generales, objeto, ámbito de aplicación y definición de determinados términos y conceptos, el Título I aborda los Principios sobre los que debe sustentarse el tratamiento de datos personales, el Título II se refiere a los derechos de los titulares de los datos (derechos ARCO), el Título III aborda la utilización de datos personales relacionados con obligaciones de carácter económico, financiero, bancario o comercial, el Título IV se refiere al tratamiento de datos por organismos públicos, el Título V trata la responsabilidad por las infracciones a la ley y el Título final modifica el Código Sanitario, otorgando la calidad de dato reservado a las recetas médicas, exámenes de laboratorio y servicios relacionados con la salud.

La ley aborda de manera amplia el tratamiento de datos de carácter personal, cualquiera sea el procedimiento, manual o automatizado, que se utilice, sea en registros o bancos de datos por organismos públicos o por particulares.

El artículo 2 de la ley aborda diversos términos y su conceptualización, así en cuanto a los sujetos que regula, distingue entre el titular de los datos, como aquella persona natural a la que se refieren los datos de carácter personal, y responsable del registro o banco de datos, como aquella persona natural o jurídica privada, o el respectivo organismo público, a quien compete las decisiones relacionadas con el tratamiento de datos. Además, define los datos de carácter personal, los datos sensibles, el dato caduco, el tratamiento de datos, el dato estadístico y el almacenamiento de datos, entre otros términos.

---

del RGPD. También se distingue entre el operador, que es el responsable del tratamiento de datos en nombre del controlador.

[410] Su nombre se debe a que el proyecto original tenía por objeto regular las intromisiones ilegales a la vida privada de las personas, refiriéndose su Título II original a la protección de datos de carácter personal, sin embargo, durante su tramitación legislativa, en el segundo tramite constitucional, su contenido se focalizó exclusivamente en la protección de datos, manteniendo la ley su nombre original. Ver Historia de la Ley 19.628:http://www.bcn.cl/leychile/Navegar/scripts/obtienearchivo?id=recursoslegales/10221.3/2468/7/HL19628.pdf

La ley chilena da cuenta de sus principales déficits en cuanto a las fuentes accesibles al público, al no considerar la licitud como presupuesto que habilite el tratamiento de datos, bastando que el acceso a la información no esté restringido[411].

Del artículo 4[412] de la ley chilena es posible colegir la importancia del consentimiento del titular para el tratamiento de sus datos de carácter personal, así como la finalidad que se persigue con el tratamiento de los datos, además de la formalidad que debe cumplir esa autorización, la que debe constar por escrito, por lo que debe ser una manifestación de voluntad explícita e inequívoca.

También la ley en su artículo 10 se refiere a los datos sensibles, los que no pueden ser objeto de tratamiento salvo cuando la ley lo autorice, exista consentimiento del titular o sean datos necesarios para la determinación u otorgamiento de beneficios de salud que correspondan a sus titulares.

La ley también dispone como excepciones al consentimiento que habilite el tratamiento de datos de carácter personal, otro precepto legal, es decir, se establecen otros habilitantes legales, tanto en los incisos 4° y 5° del artículo 4[413], como en los artículos 10[414] y 20[415].

El artículo 9 en su inciso primero aborda el principio de finalidad, al señalar que "Los datos personales deben utilizarse sólo para los fines para los cuales hubieren sido recolectados, salvo que provengan o se hayan recolectado de fuentes accesibles al público". Luego, el inciso final del mismo artículo introducido por la Ley 20.575[416], dispone que se prohíbe la realización de todo tipo de predicciones o evaluaciones de riesgo comercial que no estén basadas únicamente en información objetiva relativa a las morosidades o protestos de las personas naturales o jurídicas de las cuales se informa. La infracción a esta prohibición obligará a la eliminación

---

411 En efecto la letra i) del artículo 2 dispone: "Fuentes accesibles al público, los registros o recopilaciones de datos personales, públicos o privados, de acceso no restringido o reservado a los solicitantes".

412 "El tratamiento de los datos personales sólo puede efectuarse cuando esta ley u otras disposiciones legales lo autoricen o el titular consienta expresamente en ello. La persona que autoriza debe ser debidamente informada respecto del propósito del almacenamiento de sus datos personales y su posible comunicación al público. La autorización debe constar por escrito…"

413 "No requiere autorización el tratamiento de datos personales que provengan o que se recolecten de fuentes accesibles al público, cuando sean de carácter económico, financiero, bancario o comercial, se contengan en listados relativos a una categoría de personas que se limiten a indicar antecedentes tales como la pertenencia del individuo a ese grupo, su profesión o actividad, sus títulos educativos, dirección o fecha de nacimiento, o sean necesarios para comunicaciones comerciales de respuesta directa o comercialización o venta directa de bienes o servicios. Tampoco requerirá de esta autorización el tratamiento de datos personales que realicen personas jurídicas privadas para el uso exclusivo suyo, de sus asociados y de las entidades a que están afiliadas, con fines estadísticos, de tarificación u otros de beneficio general de aquéllos".

414 "Artículo 10. No pueden ser objeto de tratamiento los datos sensibles, salvo cuando la ley lo autorice, exista consentimiento del titular o sean datos necesarios para la determinación u otorgamiento de beneficios de salud que correspondan a sus titulares".

415 "Artículo 20. El tratamiento de datos personales por parte de un organismo público sólo podrá efectuarse respecto de las materias de su competencia y con sujeción a las reglas precedentes. En esas condiciones, no necesitará el consentimiento del titular".

416 Esta ley publicada en el Diario Oficial el 14 de febrero del 2012 establece el Principio de Finalidad en el Tratamiento de datos Personales. Ver en: https://www.leychile.cl/Navegar?idNorma=1037366&r=1 consulta realizada el 24 de julio de 2020.

inmediata de dicha información por parte del responsable de la base de datos y dará lugar a la indemnización de perjuicios que corresponda.

Sobre el cuidado y responsabilidad de los datos se refiere el artículo 11 de la ley[417], los que deben ser cuidados con la "debida diligencia", sin explicitar qué significa aquello o sobre qué principios o directrices deben ser considerados para cumplir con el mandato del legislador.

El Título II de la ley regula los denominados derechos ARCO, distinguiendo entre los derechos de acceso, rectificación, cancelación y oposición. A continuación, y en el mismo Título entre los artículos 16 y siguientes la legislación chilena establece un mecanismo de tutela a la protección de datos, el *habeas data.*

A diferencia de lo que ocurre en el ámbito europeo y también en otros países de Latinoamérica, el procedimiento de *habeas data* en Chile no se sustancia ante una autoridad administrativa o entidad de control, la que por otro lado es inexistente al día de hoy. Lo que se constata como una de las mayores debilidades del sistema chileno para el adecuado resguardo del titular de datos personales.

Así pues, en Chile, el control de legalidad en el tratamiento de datos se efectúa de forma represiva o *a posteriori* por parte del titular de los datos, ejerciendo los derechos que le concede la ley ante los responsables de los bancos de datos, ya sean estos entidades privadas o públicas, o en su defecto, ante los Tribunales de Justicia mediante el ejercicio por parte del afectado de la acción de *habeas data* que, como se señaló, está regulada en el artículo 16 de la Ley 19.628.

El recurso de *habeas data* puede revestir dos modalidades: una preventiva, cuando tenga por objeto permitir al titular de los datos personales ser informado sobre la existencia de bancos o registros de datos que contengan información que le concierne y si así fuese, acceder a los mismos; y una correctiva, cuando a través de él se exige que determinados datos personales sean corregidos, bloqueados, cancelados, pues el tratamiento que se hace de ellos es indebido, en el sentido que vulnera o conculca sus derechos. Así entonces, el *habeas data* se configura como el instrumento a través del cual los titulares de datos pueden ver protegidos sus derechos frente a acciones que resulten ilegales o arbitrarias o que importen un uso indebido de información de carácter personal que le concierne por parte del responsable del fichero o banco de datos.

Las causales de procedencia del *habeas data* están principalmente establecidas en el artículo 16 de la Ley 19.628, pero también algunas se encuentran en otras disposiciones, sistematizándolas, se pueden distinguir las siguientes causales de procedencia:

1. Que el responsable del registro o banco de datos no se pronunciare sobre una solicitud de información, modificación, bloqueo, cancelación o eliminación de datos personales dentro de dos días hábiles (contados desde la solicitud del requirente).
2. Que el responsable del registro o banco de datos denegare una solicitud de información, modificación, bloqueo, cancelación o eliminación de datos personales por una causa distinta de la seguridad de la nación o interés nacional.

[417] "Artículo 11.- El responsable de los registros o bases donde se almacenen datos personales con posterioridad a su recolección deberá cuidar de ellos con la debida diligencia, haciéndose responsable de los daños".

3. Que el responsable del registro o banco de datos denegare una solicitud de información, modificación, bloqueo, cancelación o eliminación de datos personales por motivos de seguridad de la nación o el interés nacional.
4. Por infracciones a los artículos 17 y 18 de esta misma ley, que regulan los plazos y la forma en que pueden comunicarse a terceros por los responsables de los registros o bancos de datos de carácter económico, financiero, bancario o comercial.
5. Por infracciones no contempladas en los artículos 16 y 19, según lo dispuesto en el inciso (apartado) 2°del artículo 23 de la misma ley.

El órgano jurisdiccional competente para conocer de este recurso es el Juez Civil, correspondiente al domicilio del responsable del banco de datos (o fichero de datos en la denominación del RGPD), lo que sigue la regla general en el sistema chileno, en materia de competencia de los tribunales de justicia para conocer y juzgar los asuntos controvertidos sometidos a su conocimiento, en el sentido de que la demanda se presenta en el tribunal correspondiente al domicilio del demandado. Un alternativa a la determinación del tribunal competente para conocer del *habeas data* hubiese sido el Juez del domicilio del afectado, o incluso entregar la posibilidad al titular del derecho de protección de datos, de elegir entre este y el del domicilio del demandado, ya que hay que considerar, que en el caso chileno la regla general es que los domicilios de los responsables de bancos de datos se encuentran en la Región Metropolitana, lo que eventualmente dificulta la presentación del *habeas data* si el afectado tiene su domicilio o residencia en una región distinta del país[418].

Como es evidente, el sujeto o legitimado activo para interponer el *habeas data* es el titular o interesado que ha visto vulnerado su derecho de tratamiento de datos personales previstos en la ley 19.628, el legitimado pasivo de este recurso es el responsable del banco de datos, ya sea un ente privado o un organismo público. El artículo 14[419] de la ley señala que en el evento en que los datos personales estén en un banco de datos al cual tienen acceso diversos organismos, el titular puede requerir información a cualquiera de ellos, razón por la cual, podrán ser sujetos pasivos de la acción de *habeas data* dos o más organismos públicos.

En relación con el procedimiento, la ley establece un procedimiento general principalmente contenido en el artículo 16, que establece que el *habeas data* puede ser sustentado sobre la base de:

1) La falta de pronunciamiento por parte del responsable del banco de datos dentro de los dos días hábiles siguientes al requerimiento presentado por el titular de los datos, o bien denegase la información por una causal distinta de la seguridad de la nación o el interés nacional.

2) La contravención a los artículos 17 y 18 de la ley 19.628.

[418] Esto se abordó en la discusión legislativa de la ley, como da cuenta el Boletín N° 896-07, Informe de la Comisión Mixta relativo al proyecto de ley sobre protección de datos de carácter personal.

[419] "Si los datos personales están en un banco de datos al cual tienen acceso diversos organismos, el titular puede requerir información a cualquiera de ellos".

Respecto de estas causales se procede de la siguiente manera, se debe presentar una reclamación ante el Tribunal Civil la que debe contener: indicación clara de la infracción cometida y los hechos que la configuran, además de los medios de prueba que la acreditan. Este recurso se notifica por cédula en el domicilio del responsable del banco de datos correspondiente, por su parte, el responsable del banco de datos deberá contestar dentro de quinto día hábil, formulando sus descargos y adjuntando los medios de prueba respectivos.

Si no dispone de dichos medios de prueba deberá así indicarlo, ahora bien, si ofrece prueba el tribunal fijará una audiencia, para dentro de quinto día hábil a fin de recibir la prueba ofrecida y no acompañada. Esta facultad que se le entrega al demandado, de la cual no goza el reclamante o afectado, constituye uno de los aspectos más cuestionables de este procedimiento, por cuanto vulnera el principio de la bilateralidad de la audiencia, al dejar en manos del responsable del banco de datos, la posibilidad de que exista una audiencia de prueba, ya que, si no la ofrece, no existirá tal audiencia.

La sentencia definitiva se dictará dentro de tercer día de vencido el plazo para presentar descargos, se hayan o no presentado. Ahora bien, si el tribunal decretó una audiencia de prueba, este plazo correrá una vez vencido el plazo fijado para esta.

La sentencia definitiva se notifica por cédula y es apelable en ambos efectos. El recurso deberá interponerse en el término fatal de cinco días, contado desde la notificación de la parte que lo entabla, deberá contener los fundamentos de hecho y de derecho en que se apoya y las peticiones concretas que se formulan.

Deducida la apelación, el tribunal elevará de inmediato los autos a la Corte de Apelaciones respectiva. Recibidos los autos en la Secretaría de la Corte, el Presidente ordenará dar cuenta preferente del recurso, sin esperar la comparecencia de ninguna de las partes. En todo caso, si la Corte lo estima conveniente o se le solicita con fundamento plausible, podrá ordenar traer los autos en relación para oír a los abogados de las partes, caso en el cual la causa se agregará extraordinariamente a la tabla respectiva de la misma sala. El fallo que se pronuncie sobre la apelación no será susceptible de los recursos de casación.

Todas las resoluciones, con excepción de la sentencia definitiva, se dictarán en única instancia y se notificarán por el estado diario.

La Ley 19.628 consagra también otro procedimiento, que tiene como única causal que el sustento invocado para denegar la solicitud del requirente por parte del responsable del banco de datos sea la seguridad de la nación o el interés nacional. Además, el sujeto o legitimado pasivo solo pueden ser organismos públicos, por cuanto son los únicos habilitados para invocar la causal de la seguridad de la nación o el interés nacional. En este caso el procedimiento es el siguiente:

La reclamación deberá deducirse ante la Corte Suprema, la que solicitará informe de la autoridad de que se trate por la vía que considere más rápida, fijándole plazo al efecto, transcurrido el cual resolverá en cuenta la controversia. La competencia radica en el máximo Tribunal de Justicia chileno, cuestión que se justificaría considerando la importancia o entidad de la causal invocada para el rechazo de la solicitud, y teniendo en cuenta, además, que el requerido o demandado será un órgano del Estado.

De recibirse prueba, se consignará en un cuaderno separado y reservado, que conservará ese carácter aun después de terminada la causa si por sentencia ejecutoriada se denegare la solicitud del requirente.

La sala de la Corte Suprema que conozca la reclamación, si lo estima conveniente o se le solicita con fundamento plausible, podrá ordenar traer los autos en relación para oír a los abogados de las partes, caso en el cual la causa se agregará extraordinariamente a la tabla respectiva de la misma sala. El Presidente del Tribunal dispondrá que la audiencia no sea pública, ya que este procedimiento reviste las características de secreto, debido a las eventuales causales invocadas.

La ley 19.628, establece también un tercer procedimiento, previsto en el artículo 23, de naturaleza sumaria, que tiene lugar cuando las infracciones a la ley sean cualquiera de las que no están previstas en los artículos 16 y 19, como por ejemplo si una entidad pública realiza tratamiento de datos personales sin estar habilitada o tener competencia para ello, si el responsable de los datos no informa a terceros que dichos datos se han modificado o eliminado.

Las sanciones previstas en esta ley son pecuniarias y se harán efectivas en caso de acogerse la reclamación. La misma sentencia fijará un plazo prudencial para dar cumplimiento a lo resuelto y podrá aplicar una multa de 1 a 10 unidades tributarias mensuales o de 10 a 50 unidades tributarias mensuales. Finalmente, indica la ley, que la falta de entrega oportuna de la información o el retardo en efectuar la modificación, en la forma que decrete el Tribunal, serán castigados con multa de 2 a 50 unidades tributarias mensuales[420] y, si el responsable del banco de datos requerido fuere un organismo público, el tribunal podrá sancionar al jefe del servicio con la suspensión de su cargo, por un lapso de cinco a quince días.

En lo procedimental, también hay que tener presente lo dispuesto en la parte final del artículo 23 en el sentido de que el juez tomará todas las providencias que estime convenientes para hacer efectiva la protección de los derechos que esta ley establece, que la prueba se apreciará en conciencia por el juez y que el monto de la indemnización será establecido prudencialmente por el juez, considerando las circunstancias del caso y la gravedad de los hechos.

Precisamente, la acción de indemnización de perjuicios a la que el legislador hace referencia puede ejercerse por tres vías: En primer lugar, mediante el procedimiento que dispone el artículo 23, donde la acción indemnizatoria se interpone conjuntamente con la reclamación o habeas data. En segundo lugar, puede interponerse esta acción indemnizatoria ante los tribunales civiles en juicio ordinario de mayor cuantía según las reglas generales del procedimiento civil chileno. Y, en tercer lugar, la acción indemnizatoria puede interponerse en juicio sumario, ya que se establece una regla residual, en la que todas las infracciones no contempladas en los artículos 16 y 19, incluida la indemnización de los perjuicios, se sujetarán al procedimiento sumario.

Por último, como ya se señaló, el artículo 11[421] de la ley, establece que el responsable de los registros o bancos donde se almacenen datos personales con posterioridad a su recolección deberá cuidar de ellos con la debida diligencia, haciéndose responsable de los daños. Y el artículo 23, indica que el responsable del tratamiento de datos ya sea un particular o un

[420] La Unidad Tributaria Mensual (UTM): Unidad definida en Chile que corresponde a un monto de dinero expresado en pesos y determinado por ley, el cual se actualiza en forma permanente por el Índice de Precios al Consumidor (IPC) y se utiliza como medida tributaria. 1 UTM equivale a poco menos de 55 euros; 10 UTM equivalen a 547 euros y 50 UTM equivalen a 2.820 euros al 29 de octubre de 2021.

[421] "El responsable de los registros o bases donde se almacenen datos personales con posterioridad a su recolección deberá cuidar de ellos con la debida diligencia, haciéndose responsable de los daños".

organismo público, debe indemnizar el daño patrimonial y moral que causare por el tratamiento indebido de los datos.

Cuando la ley se refiere a "tratamiento indebido de los datos" o a "debida diligencia", se advierte que se exige culpa o negligencia en el actuar del responsable de datos, por lo que se siguen las reglas generales en materia de responsabilidad civil existentes en el ordenamiento jurídico chileno[422].

Una nueva ley de protección de datos personales está actualmente en tramitación en el Congreso chileno, sus principales alcances serán abordados en otro capítulo de este trabajo, solo a modo de referencia inicial es posible afirmar que este proyecto de ley se encuentra influenciado por el RGPD y propone una nueva institucionalidad para la protección de datos en Chile[423] instalando una autoridad de control en la materia que sea la instancia de naturaleza administrativa, donde primero se pueda interponer una reclamación por parte del titular afectado por el indebido tratamiento de sus datos de carácter personal.

Colombia

La norma colombiana que regula la protección de datos de carácter personal, esta contendida en la Ley Estatutaria N° 1581 del 17 de octubre de 2012[424], la que se estructura sobre IX Títulos y treinta artículos, el Título I aborda el "Objeto, Ámbito de aplicación y Definiciones", el Título II trata los "Principios Rectores", el Título III se refiere a las "Categorías especiales de datos", el Título IV regula los "Derechos y condiciones de legalidad para el Tratamiento de Datos", el Título V se refiere al "Procedimiento", el Título VI se refiere a los "Deberes de los Responsables del Tratamiento y del Encargado del Tratamiento", el Título VII aborda "Los Mecanismos de Vigilancia y Sanción" y se divide en tres capítulos. El Capítulo uno se denomina "De la Autoridad de Control", el Capítulo dos se refiere al "Procedimiento y Sanciones", el Capítulo tres se refiere al "Registro Nacional de Bases de Datos". El Título VIII se refiere a la "Transferencia de Datos a Terceros Países", y el Título IX se denomina "Otras Disposiciones".

Los artículos 1[425] y 2[426] abordan el objeto y el ámbito de aplicación de la ley respectivamente, conteniéndose también en el artículo 2 los casos en que sus disposiciones no serán aplicables, y que son:

---

[422] Esto es un régimen de responsabilidad de tipo subjetiva para determinar la responsabilidad del Estado, que se sustenta en la falta de servicio, que se configura cuando el órgano o entidad pública, no entrega el servicio debiendo hacerlo, lo hace deficitariamente o lo hace de manera tardía.

[423] Ver Boletines N° 11.144-07 y N° 11.092-07. Proyecto de ley que regula la Protección y el Tratamiento de los Datos Personales y crea la Agencia de Protección de Datos Personales: https://www.camara.cl/legislacion/ProyectosDeLey/tramitacion.aspx?prmID=11661&prmBoletin=11144-07

[424] Ver en: https://www.sic.gov.co/sites/default/files/normatividad/Ley_1581_2012.pdf. Consulta realizada el 28 de julio de 2020.

[425] "Artículo 1. Objeto. La presente ley tiene por objeto desarrollar el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bases de datos o archivos, y los demás derechos, libertades y garantías constitucionales a que se refiere el artículo 15 de la Constitución Política; así como el derecho a la información consagrado en el artículo 20 de la misma".

[426] "Artículo 2. Ámbito de aplicación. Los principios y disposiciones contenidas en la presente ley serán aplicables a los datos personales registrados en cualquier base de datos que los haga susceptibles de tratamiento por entidades

> *"a) A las bases de datos o archivos mantenidos en un ámbito exclusivamente personal o doméstico. Cuando estas bases de datos o archivos vayan a ser suministrados a terceros se deberá, de manera previa, informar al Titular y solicitar su autorización. En este caso los Responsables y Encargados de las bases de datos y archivos quedarán sujetos a las disposiciones contenidas en la presente ley; b) A las bases de datos y archivos que tengan por finalidad la seguridad y defensa nacional, así como la prevención, detección, monitoreo y control del lavado de activos y el financiamiento del terrorismo; c) A las bases de datos que tengan como fin y contengan información de inteligencia y contrainteligencia; d) A las bases de datos y archivos de información periodística y otros contenidos editoriales; e) A las bases de datos y archivos regulados por la Ley N° 1266 de 2008; y f) A las bases de datos y archivos regulados por la Ley 79 de 1993"*.

El artículo 3 se refiere a las definiciones de términos tales como; autorización, bases de datos, tratamiento y titular.

El artículo cuarto establece los Principios para el tratamiento de datos personales, distinguiendo entre, el principio de legalidad, el principio de finalidad, principio de libertad, principio de veracidad o calidad, principio de transparencia, principio de acceso y circulación restringida, principio de seguridad y principio de confidencialidad.

El artículo 5 aborda los datos sensibles, señalando que:

> *"Para los propósitos de la presente ley, se entiende por datos sensibles aquellos que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición así como los datos relativos a la salud, a la vida sexual y los datos biométricos"*.

El artículo 6 se refiere al tratamiento de datos sensibles y el artículo 7 a los derechos de niños, niñas y adolescentes.

Siguiendo a otras legislaciones que regulan la materia, la ley en su artículo 8 se refiere a los derechos de los titulares de los datos, donde se distingue entre los siguientes derechos: a) Conocer, actualizar y rectificar sus datos personales frente a los Responsables del Tratamiento o Encargados del Tratamiento. Este derecho se podrá ejercer, entre otros frente a datos parciales, inexactos, incompletos, fraccionados, que induzcan a error, o aquellos cuyo Tratamiento esté expresamente prohibido o no haya sido autorizado; b) Solicitar prueba de la autorización otorgada al Responsable del Tratamiento salvo cuando expresamente se exceptúe como requisito para el Tratamiento, de conformidad con lo previsto en el artículo 10 de la presente ley; c) Ser informado por el Responsable del Tratamiento o el Encargado del Tratamiento, previa solicitud, respecto del uso que le ha dado a sus datos personales; d) Presentar ante la Superintendencia de Industria y Comercio quejas por infracciones a lo dispuesto en la presente ley y las demás normas que la modifiquen, adicionen o complementen;

---

de naturaleza pública o privada. La presente ley aplicará al Tratamiento de datos personales efectuado en territorio colombiano o cuando al Responsable del Tratamiento o Encargado del Tratamiento no establecido en territorio nacional le sea aplicable la legislación colombiana en virtud de normas y tratados internacionales".

e) Revocar la autorización y/o solicitar la supresión del dato cuando en el Tratamiento no se respeten los principios, derechos y garantías constitucionales y legales. La revocatoria y/o supresión procederá cuando la Superintendencia de Industria y Comercio haya determinado que en el Tratamiento el Responsable o Encargado han incurrido en conductas contrarias a esta ley y a la Constitución; y f) Acceder en forma gratuita a sus datos personales que hayan sido objeto de Tratamiento.

El artículo 12[427] establece el deber de informar que tiene el responsable del tratamiento de datos al titular de estos, este último debe autorizar el tratamiento de sus datos de carácter personal.

Los artículos 17 y 18 regulan los deberes del responsable y del encargado respectivamente, del tratamiento de datos de carácter personal. Según el artículo 3 de la misma ley, el Encargado del Tratamiento, es la Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, realice el Tratamiento de datos personales por cuenta del Responsable del Tratamiento. Y el Responsable del Tratamiento es la Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, decida sobre la base de datos y/o el Tratamiento de los datos.

La ley N° 1.581, entre los artículos 19 al 24, regula la autoridad de control en materia de protección de datos, que es la Superintendencia de Industria y Comercio y más concretamente la Delegatura para la Protección de Datos Personales, así como las funciones que tiene, los procedimientos que deberá sustanciar y las sanciones que se encuentra facultada para aplicar.

El artículo 25 dispone la existencia de un Registro Nacional de Bases de Datos, que es el directorio público de las bases de datos sujetas a Tratamiento que operan en Colombia. El registro es administrado por la Superintendencia de Industria y Comercio y es de libre consulta para los ciudadanos. Para realizar el registro de bases de datos, los interesados deberán aportar a la Superintendencia las políticas de tratamiento de la información, las cuales obligarán a los responsables y encargados de este, y cuyo incumplimiento acarreará las sanciones correspondientes. Las políticas de Tratamiento en ningún caso podrán ser inferiores a los deberes contenidos en la ley.

Por último, el artículo 26 de la ley colombiana regula la transferencia internacional de datos, estableciendo que se prohíbe la transferencia de datos de cualquier tipo a países que no proporcionen niveles adecuados de protección de datos. El legislador estima que un país ofrece un nivel adecuado de protección de datos cuando cumple con los estándares fijados por la Superintendencia de Industria y Comercio sobre la materia, los cuales en ningún caso podrán ser inferiores a los que esta ley exige.

Además se establecen las excepciones a dicha prohibición, las que tienen lugar en los siguientes casos: a) Cuando se trate de información respecto de la cual el titular haya otorgado su autorización expresa e inequívoca para la transferencia; b) Cuando el intercambio de datos sea de carácter médico o cuando así lo exija el tratamiento del titular por razones de salud o

[427] "El Responsable del Tratamiento, al momento de solicitar al Titular la autorización, deberá informarle de manera clara y expresa lo siguiente: a) El Tratamiento al cual serán sometidos sus datos personales y la finalidad del mismo. b) El carácter facultativo de la respuesta a las preguntas que le sean hechas, cuando éstas versen sobre datos sensibles o sobre los datos de las niñas, niños y adolescentes. c) Los derechos que le asisten como Titular. d) La identificación, dirección física o electrónica y teléfono del Responsable del Tratamiento".

higiene pública; c) Cuando se trate de transferencias bancarias o bursátiles, conforme a la legislación que les resulte aplicable; d) En el caso de transferencias acordadas en el marco de tratados internacionales en los cuales la República de Colombia sea parte, con fundamento en el principio de reciprocidad; e) En transferencias necesarias para la ejecución de un contrato entre el titular y el Responsable del Tratamiento, o para la ejecución de medidas precontractuales siempre y cuando se cuente con la autorización del titular; f) En transferencias legalmente exigidas para la salvaguardia del interés público, o para el reconocimiento, ejercicio o defensa de un derecho en un proceso judicial.

Finalmente, se dispone que la Superintendencia de Industria y Comercio queda facultada para autorizar la transferencia internacional de datos, realizando las diligencias tendientes a establecer si se cumplen o no los presupuestos que hacen viable la operación.

Costa Rica

El 5 de septiembre del año 2011 se publica en el diario oficial La Gaceta N° 170 la Ley N° 8.968 de 7 de julio del mismo año sobre protección de la persona frente al tratamiento de sus datos personales[428], la que fue complementada por el Reglamento contenido en el Decreto Ejecutivo N° 37554-JP del 30 de octubre del año 2012 y publicado en el alcance N° 45 del diario oficial La Gaceta del 5 de marzo del año 2013. El cual es reformado y actualizado mediante el Decreto Ejecutivo N° 40008-JP del 19 de julio del año 2016, publicado en el alcance N° 287 del diario oficial La Gaceta del 6 de diciembre del mismo año[429].

La ley sobre protección de datos costarricense se estructura sobre seis capítulos, treintaicuatro artículos y tres artículos transitorios. El Capítulo I te titula "Disposiciones Generales" y consta de tres artículos, el artículo 1 se refiere al objeto y fin[430] de la ley; el artículo 2 a su ámbito de aplicación y el artículo 3 define diversos términos.

El Capítulo II se titula "Principios y Derechos Básicos para la Protección de Datos Personales", se divide en tres secciones, la sección I regula los Principios y Derechos Básicos, en su artículo 4 se establece y reconoce la Autodeterminación Informativa, al señalar que "Toda persona tiene derecho a la autodeterminación informativa, la cual abarca el conjunto de principios y garantías relativas al legítimo tratamiento de sus datos personales..." y luego agrega: "Se reconoce también la autodeterminación informativa como un derecho fundamental, con el objeto de controlar el flujo de informaciones que conciernen a cada persona, derivado del derecho a la privacidad, evitando que se propicien acciones discriminatorias".

428

Ver:http://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_texto_completo.aspx?param1=NRTC&nValor1=1&nValor2=70975&nValor3=85989&strTipM=TC consulta realizada el 03 de agosto de 2020.

429

Ver:http://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_texto_completo.aspx?nValor1=1&nValor2=74352 consulta realizada el 03 de agosto de 2020.

430 "Esta ley es de orden público y tiene como objetivo garantizar a cualquier persona, independientemente de su nacionalidad, residencia o domicilio, el respeto a sus derechos fundamentales, concretamente, su derecho a la autodeterminación informativa en relación con su vida o actividad privada y demás derechos de la personalidad, así como la defensa de su libertad e igualdad con respecto al tratamiento automatizado o manual de los datos correspondientes a su persona o bienes".

Un aspecto para destacar es que a diferencia de otras legislaciones latinoamericanas se refiere explícitamente a la autodeterminación informativa y no solo al derecho de protección de datos personales.

Siguiendo con los principios, el artículo 5 aborda el del Consentimiento Informado, el artículo 6 se refiere al Principio de Calidad de la Información, el artículo 7 al derecho de acceso a la información y al derecho de rectificación.

La sección dos aborda las Categorías Especiales del Tratamiento de los Datos, distinguiendo el artículo 9 entre datos sensibles, datos personales de acceso restringido[431], datos personales de acceso irrestricto[432] y datos referentes al comportamiento crediticio[433].

La sección tres del Capítulo II aborda la Seguridad y Confidencialidad del Tratamiento de los Datos. Señalando el artículo 10 a propósito de la seguridad de los datos que: "El responsable de la base de datos deberá adoptar las medidas de índole técnica y de organización necesarias para garantizar la seguridad de los datos de carácter personal y evitar su alteración, destrucción accidental o ilícita, pérdida, tratamiento o acceso no autorizado, así como cualquier otra acción contraria a esta ley. Dichas medidas deberán incluir, al menos, los mecanismos de seguridad física y lógica más adecuados de acuerdo con el desarrollo tecnológico actual, para garantizar la protección de la información almacenada. No se registrarán datos personales en bases de datos que no reúnan las condiciones que garanticen plenamente su seguridad e integridad, así como la de los centros de tratamiento, equipos, sistemas y programas. Por vía de reglamento se establecerán los requisitos y las condiciones que deban reunir las bases de datos automatizadas y manuales, y de las personas que intervengan en el acopio, almacenamiento y uso de los datos".

El Capítulo III se titula "Transferencias de Datos Personales", que en su artículo 14 dispone a propósito de la transferencia de datos personales, como regla general, que: "Los responsables de las bases de datos, públicas o privadas, solo podrán transferir datos contenidos en ellas cuando el titular del derecho haya autorizado expresa y válidamente tal transferencia y se haga sin vulnerar los principios y derechos reconocidos en esta ley".

El Capítulo IV regula la "Agencia de Protección de Datos de los Habitantes", a la que también hace referencia como "Prodhab", este capítulo se divide en dos secciones, la Sección I regula las disposiciones generales, donde su artículo 16 se refiere a las atribuciones de la Agencia, el artículo 17 a la dirección de esta, el artículo 18 a su personal, el artículo 19 a las prohibiciones de sus funcionarios y el artículo 20 a su presupuesto. La sección II del Capítulo IV se refiere a

---

[431] "Datos personales de acceso restringido son los que, aun formando parte de registros de acceso al público, no son de acceso irrestricto por ser de interés solo para su titular o para la Administración Pública. Su tratamiento será permitido únicamente para fines públicos o si se cuenta con el consentimiento expreso del titular".

[432] "Datos personales de acceso irrestricto son los contenidos en bases de datos públicas de acceso general, según lo dispongan las leyes especiales y de conformidad con la finalidad para la cual estos datos fueron recabados. No se considerarán contemplados en esta categoría: la dirección exacta de la residencia, excepto si su uso es producto de un mandato, citación o notificación administrativa o judicial, o bien, de una operación bancaria o financiera, la fotografía, los números de teléfono privados y otros de igual naturaleza cuyo tratamiento pueda afectar los derechos y los intereses de la persona titular".

[433] "Los datos referentes al comportamiento crediticio se regirán por las normas que regulan el Sistema Financiero Nacional, de modo que permitan garantizar un grado de riesgo aceptable por parte de las entidades financieras, sin impedir el pleno ejercicio del derecho a la autodeterminación informativa ni exceder los límites de esta ley".

la Estructura Interna de la Agencia, disponiendo el artículo 21 el Registro de Archivo y Bases de Datos al señalar su inciso 1° que: "Toda base de datos, pública o privada, administrada con fines de distribución, difusión o comercialización, debe inscribirse en el registro que al efecto habilite la Prodhab. La inscripción no implica el trasvase o la transferencia de los datos".

El Capítulo V se titula "Procedimientos", en su artículo 24 se dispone que "Cualquier persona que ostente un derecho subjetivo o un interés legítimo puede denunciar, ante la Prodhab, que una base de datos pública o privada actúa en contravención de las reglas o los principios básicos para la protección de los datos y la autodeterminación informativa establecidas en esta ley". El artículo 27 se refiere al procedimiento sancionatorio y el 28 a las sanciones, siendo todas de contenido pecuniario[434]. Entre los artículos 29, 30 y 31 se consagran los distintos tipos de faltas, faltas leves, faltas graves y faltas gravísimas respectivamente.

La Sección III del Capítulo V regula los procedimientos internos señalando el artículo 32 en relación con el Régimen sancionatorio para bases de datos públicas, que: "Cuando la persona responsable de una base de datos pública cometa alguna de las faltas anteriores, la Prodhab dictará una resolución estableciendo las medidas que proceda adoptar para que cesen o se corrijan los efectos de la falta. Esta resolución se notificará a la persona responsable de la base de datos, al órgano del que dependa jerárquicamente y a los afectados, si los hay. La resolución podrá dictarse de oficio o a petición de parte. Lo anterior sin perjuicio de la responsabilidad penal en que haya incurrido".

Ecuador

El 26 mayo del año 2021 entra en vigor la Ley Orgánica de Protección de Datos Personales del Ecuador[435] (LOPDP), cuya tramitación legislativa demoro menos de dos años[436], esta ley se estructura sobre la base de doce capítulos, setenta y siete artículos, un apartado sobre "Disposiciones Generales" con ocho artículos, otro apartado sobre "Disposiciones Transitorias" con cuatro artículos y dos apartados finales sobre "Disposiciones Reformatorias" y "Disposiciones Derogatorias", con cuatro artículos cada uno.

El Capítulo I se refiere al Ámbito de aplicación integral de la ley; el Capítulo II aborda los Principios; el Capítulo III trata sobre los Derechos; el Capítulo IV regula las Categorías Especiales de Datos; el Capítulo V se refiere a la Transparencia o Comunicación y Acceso a Datos Personales por Terceros; el Capítulo VI aborda la Seguridad de Datos Personales; el Capítulo VII trata Del Responsable, Encargado y Delegado de Protección de Datos Personales; el Capítulo VIII se refiere a la Responsabilidad Proactiva; el Capítulo IX aborda la

[434] "Si se ha incurrido en alguna de las faltas tipificadas en esta ley, se deberá imponer alguna de las siguientes sanciones, sin perjuicio de las sanciones penales correspondientes: a) Para las faltas leves, una multa hasta de cinco salarios base del cargo de auxiliar judicial I, según la Ley de Presupuesto de la República; b) Para las faltas graves, una multa de cinco a veinte salarios base del cargo de auxiliar judicial I, según la Ley de Presupuesto de la República; c) Para las faltas gravísimas, una multa de quince a treinta salarios base del cargo de auxiliar judicial I, según la Ley de Presupuesto de la República, y la suspensión para el funcionamiento del fichero de uno a seis meses".

[435] Ver en: ro-459-5to-sup-26-05-2021.pdf (asambleanacional.gob.ec)

[436] En efecto, esta ley se presentó como una iniciativa de proyecto de ley el 19 de septiembre del año 2019, por parte del entonces Presidente de la República del Ecuador Lenin Moreno, cuyos antecedentes materiales estuvieron en la mayor filtración de datos ocurrida en ese país que involucro a diversas instituciones públicas.

Transferencia o Comunicación Internacional de Datos Personales; el Capítulo X trata De los Requisitos Directos y de la Gestión del Procedimiento Administrativo; el Capítulo XI se refiere a las Medidas Correctivas, Infracciones y Régimen Sancionatorio; y el Capítulo XII regula la Autoridad de Protección de Datos Personales.

El artículo 1 de la ley se refiere a su objeto y finalidad, cual es "garantizar el ejercicio del derecho a la protección de datos personales, que incluye el acceso y decisión sobre información y datos de este carácter, así como su correspondiente protección. Para dicho efecto regula, prevé y desarrolla principios, derechos, obligaciones y mecanismos de tutela".

De igual forma los artículos 2 y 3 se refieren al ámbito de aplicación material y al ámbito de aplicación territorial respectivamente. El artículo cuarto de la ley, al igual que lo hacen otras legislaciones análogas se refiere a una serie de "Términos y definiciones".

> *Artículo 2 de la LOPDP del Ecuador; "La presente ley se aplicará al tratamiento de datos personales contenidos en cualquier tipo de soporte, automatizados o no, así como a toda modalidad de uso posterior. La ley no será aplicable a: a) Personas naturales que utilicen estos datos en la realización de actividades familiares o domésticas; b) Personas fallecidas, sin perjuicio de lo establecido en el artículo 28 de la presente Ley; c) Datos anonimizados, en tanto no sea posible identificar a su titular. Tan pronto los datos dejen de estar disociados o de ser anónimos, su tratamiento estará sujeto al cumplimiento de las obligaciones de esta ley, especialmente la de contar con una base de licitud para continuar tratando los datos de manera no anonimizada o disociada; d) Actividades periodísticas y otros contenidos editoriales; e) Datos personales cuyo tratamiento se encuentre regulado en normativa especializada de igual o mayor jerarquía en materia de gestión de riesgos por desastres naturales; y, seguridad y defensa del Estado, en cualquiera de estos casos deberá darse cumplimiento a los estándares internacionales en la materia de derechos humanos y a los principios de esta ley, y como mínimo a los criterios de legalidad, proporcionalidad y necesidad; f) Datos o bases de datos establecidos para la prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, llevado a cabo por los organismos estatales competentes en cumplimiento de sus funciones legales. En cualquiera de estos casos deberá darse cumplimiento a los estándares internacionales en la materia de derechos humanos y a los principios de esta ley, y como mínimo a los criterios de legalidad, proporcionalidad y necesidad; y g) Datos que identifican o hacen identificable a personas jurídicas.*
>
> *Son accesibles al público y susceptibles de tratamiento los datos personales referentes al contacto de profesionales y los datos de comerciantes, representantes y socios y accionistas de personas jurídicas y servidores públicos, siempre y cuando se refieran al ejercicio de su profesión, oficio, giro de negocio, competencias, facultades, atribuciones o cargo y se trate de nombres y apellidos, funciones o puestos desempeñados, dirección postal o electrónica, y, número de teléfono profesional. En el caso de los servidores públicos, además serán de acceso público y susceptibles de tratamiento de datos, el histórico y vigente de la declaración patrimonial y de su remuneración".*

> *Artículo 3 de la LOPDP del Ecuador; "Sin perjuicio de la normativa establecida en los instrumentos internacionales ratificados por el Estado ecuatoriano que versen sobre esta materia, se aplicará la presente Ley cuando: 1. El tratamiento de datos personales se realice en cualquier parte del territorio nacional; 2. El responsable o encargado del tratamiento de datos personales se encuentre domiciliado en cualquier parte del territorio nacional; 3. Se realice tratamiento de datos personales de titulares que residan en el Ecuador por parte de un responsable o encargado no establecido en el Ecuador, cuando las actividades del tratamiento estén relacionadas con: 1) La oferta de bienes o servicios a dichos titulares, independientemente de si a estos se les requiere su pago, o, 2) del control de su comportamiento, en la medida en que este tenga lugar en el Ecuador; y, 4. Al responsable o encargado del tratamiento de datos personales, no domiciliado en el territorio nacional, le resulte aplicable la legislación nacional en virtud de un contrato o de las regulaciones vigentes del derecho internacional público"*.

El artículo cinco de la ley estructura lo que denomina un sistema de protección de datos personales, integrado por: 1) el Titular; 2) el Responsable del tratamiento; 3) el Encargado del tratamiento; 4) el Destinatario; 5) la Autoridad de Protección de Datos Personales; y, 6) el Delegado de protección de datos personales.

El artículo diez se refiera a los principios que sustentan y rigen la ley de protección de datos, donde se distinguen los principios de Juridicidad, Lealtad, Transparencia, Pertinencia y minimización de datos personales, Proporcionalidad del tratamiento, Confidencialidad, Calidad y exactitud, Seguridad de datos personales, Responsabilidad proactiva y demostrada, Aplicación favorable al titular e Independencia del control.

Un eje central en la legislación ecuatoriana es el Principio de Responsabilidad proactiva y demostrada en virtud del cual el responsable del tratamiento de datos personales deberá acreditar el haber implementado mecanismos para la protección de datos personales; es decir, el cumplimiento de los principios, derechos y obligaciones establecidos en la Ley, para lo cual, además de la normativa aplicable, podrá valerse de estándares, mejores prácticas, esquemas de autorregulación, así como códigos de protección, sistemas de certificación, sellos de protección de datos personales o cualquier otro mecanismo que se determine adecuado a los fines, la naturaleza del dato personal o el riesgo del tratamiento.

En el capítulo III de la ley, relativo a los Derechos, destaca el establecimiento del Derecho a la portabilidad, expresión de la influencia que tuvo el RGPD de la UE sobre la reciente legislación ecuatoriana, el artículo diecisiete de la ley se refiere al derecho a la portabilidad reconociendo que el titular tiene el derecho a recibir del responsable del tratamiento, sus datos personales en un formato compatible, actualizado, estructurado, común, interoperable y de lectura mecánica, preservando sus características; o a transmitirlos a otros responsables. Debiendo la Autoridad de Protección de Datos Personales dictar la normativa para el ejercicio del derecho a la portabilidad.

El titular podrá solicitar que el responsable del tratamiento realice la transferencia o comunicación de sus datos personales a otro responsable del tratamiento en cuanto fuera técnicamente posible y sin que el responsable pueda aducir impedimento de cualquier orden con el fin de ralentizar el acceso, la transmisión o reutilización de datos por parte del titular o de otro responsable del tratamiento. Luego de completada la transferencia de datos, el

responsable que lo haga procederá a su eliminación, salvo que el titular disponga su conservación.

Para que proceda el derecho a la portabilidad de datos es necesario que se produzca al menos una de las siguientes condiciones: 1) Que el titular haya otorgado su consentimiento para el tratamiento de sus datos personales para uno o varios fines específicos. La transferencia o comunicación se hará entre responsables del tratamiento de datos personales cuando la operación sea técnicamente posible; en caso contrario los datos deberán ser transmitidos directamente al titular; 2) Que el tratamiento se efectúe por medios automatizados; 3) Que se trate de un volumen relevante de datos personales, según los parámetros definidos en el reglamento de la ley; o, 4) Que el tratamiento sea necesario para el cumplimiento de obligaciones y el ejercicio de derechos del responsable o encargado del tratamiento de datos personales, o del titular en el ámbito del derecho laboral y seguridad social. Esta transferencia o comunicación debe ser económica y financieramente eficiente, expedita y sin trabas.

La ley ecuatoriana también dispone que no procederá el derecho a la portabilidad cuando se trate de información inferida, derivada, creada, generada u obtenida a partir del análisis o tratamiento efectuado por el responsable del tratamiento de datos personales con base en los datos personales proporcionados por el titular, como es el caso de los datos personales que hubieren sido sometidos a un proceso de personalización, recomendación, categorización o creación de perfiles.

Otro aspecto distintivo de los contenidos de la legislación sobre protección de datos ecuatoriana es el de la consagración del Derecho a la educación digital[437], como aquel en que "Las personas tienen derecho al acceso y disponibilidad del conocimiento, aprendizaje, preparación, estudio, formación, capacitación, enseñanza e instrucción relacionados con el uso y maneje adecuado sano, constructivo, seguro y responsable de las tecnologías de la información y comunicación, en estricto apego a la dignidad e integridad humana, los derechos fundamentales y libertades individuales con especial énfasis en la intimidad, la vida privada, autodeterminación informativa, identidad y reputación en línea, ciudadanía digital y el derecho a la protección de datos personales, así como promover una cultura sensibilizada en el derecho de protección de datos personales.

El derecho a la educación digital tendrá un carácter inclusivo sobre todo en lo que respecta a las personas con necesidades educativas especiales. El sistema educativo nacional, incluyendo el sistema de educación superior, garantizará la educación digital no solo a favor de los estudiantes de todos los niveles sino también de los docentes, debiendo incluir dicha temática en su proceso de formación".

El Salvador

Si bien en El Salvador no existe una ley específica sobre protección de datos de carácter personal, la Ley de Acceso a la Información Pública contenida en el Decreto Legislativo N° 534, de fecha 02 de diciembre de 2010, publicado en el Diario Oficial N° 70, Tomo N° 391, de fecha 08 de abril de 2011, en su Título III aborda los datos personales. Antes, eso sí, en su artículo 6 letras a y b, conceptualiza los datos personales y los datos personales sensibles. Dispone que los datos personales son "la información privada concerniente a una persona,

[437] Artículo 23 de la LOPDP del Ecuador.

identificada o identificable, relativa a su nacionalidad, domicilio, patrimonio, dirección electrónica, número telefónico u otra análoga". Y que los datos personales sensibles son "los que corresponden a una persona en lo referente al credo, religión, origen étnico, filiación o ideologías políticas, afiliación sindical, preferencias sexuales, salud física y mental, situación moral y familiar y otras informaciones íntimas de similar naturaleza o que pudieran afectar el derecho al honor, a la intimidad personal y familiar y a la propia imagen".

El Título III consta de dos capítulos, el primero se titula "Protección de datos Personales", donde se establece el derecho a la protección de datos, específicamente en el artículo 31, el cual dispone: "Toda persona, directamente o a través de su representante, tendrá derecho a saber si se están procesando sus datos personales; a conseguir una reproducción inteligible de ella sin demora; a obtener las rectificaciones o supresiones que correspondan cuando los registros sean injustificados o inexactos y a conocer los destinatarios cuando esta información sea transmitida, permitiéndole conocer las razones que motivaron su petición, en los términos de esta ley. El acceso a los datos personales es exclusivo de su titular o su representante".

Como se puede observar, si bien la Constitución salvadoreña no hace un reconocimiento explícito del derecho a la protección de datos, si se hace a nivel legislativo, eso sí, este reconocimiento tiene lugar en un precepto que fundamentalmente regula el acceso a la información pública.

El artículo 32 se refiere a los deberes que deberán asumir las entidades responsables de tutelar los datos personales, los que se constituyen como una especie de derecho de los titulares de los datos al establecer que dichas entidades deberán: a. Adoptar procedimientos adecuados para recibir y responder las solicitudes de indagatoria, actualización, modificación y supresión de datos personales; b. Usar los datos exclusivamente en el cumplimiento de los fines institucionales para los que fueron solicitados u obtenidos; c. Procurar que los datos personales sean exactos y actualizados; d. Rectificar o completar los datos personales que fueren inexactos o incompletos; e. Adoptar medidas que protejan la seguridad de los datos personales y eviten su alteración, pérdida, transmisión y acceso no autorizado.

De igual forma el artículo 33 prohíbe la difusión de los datos o antecedentes, sin el consentimiento de su titular al establecer que "Los entes obligados no podrán difundir, distribuir o comercializar los datos personales contenidos en los sistemas de información administrados en el ejercicio de sus funciones, salvo que haya mediado el consentimiento expreso y libre, por escrito o por un medio equivalente, de los individuos a que haga referencia la información".

Luego, el artículo 34 consagra las excepciones a la difusión de los datos, aun cuando no mediare consentimiento de su titular; a. Cuando fuere necesario por razones estadísticas, científicas o de interés general, siempre que no se identifique a la persona a quien se refieran; b. Cuando se transmitan entre entes obligados, siempre y cuando los datos se destinen al ejercicio de sus facultades; c. Cuando se trate de la investigación de delitos e infracciones administrativas, en cuyo caso se seguirán los procedimientos previstos en las leyes pertinentes; d. Cuando exista orden judicial; e. Cuando contraten o recurran a terceros para la prestación de un servicio que demande el tratamiento de datos personales. Los terceros no podrán utilizar los datos personales con propósitos distintos a aquellos para los cuales se les hubieren proporcionado y tendrán las responsabilidades legales que genere su actuación.

En el capítulo dos del Título III, se regula el procedimiento para solicitar datos personales, al disponer el artículo 36 que los titulares de los datos personales o sus representantes, previa acreditación, podrán solicitar a los entes obligados, ya sea mediante escrito libre, en los términos o formulario expedido por el Instituto de Acceso a la Información Pública[438]: a. La información contenida en documentos o registros sobre su persona; b. Informe sobre la finalidad para la que se ha recabado tal información; c. La consulta directa de documentos, registros o archivos que contengan sus datos que obren en el registro o sistema bajo su control; d. La rectificación, actualización, confidencialidad o supresión de la información que le concierna, según sea el caso, y toda vez que el procedimiento para tales modificaciones no esté regulado por una ley especial. Tratándose de los literales a, b y c, los entes obligados deberán entregar en un plazo de diez días hábiles, contados a partir de la presentación de la solicitud, en formato comprensible para el solicitante, la información correspondiente; o bien, le comunicarán por escrito que ese registro o sistema de datos personales no contiene los requeridos por el solicitante. En el caso del literal d, la solicitud deberá ser acompañada de la documentación que respalde lo pedido.

Según el artículo 38 de la ley, si se negara la entrega de informes, de la consulta directa, rectificación, actualización, confidencialidad o supresión de datos personales, procederá la interposición del recurso de apelación ante el Instituto. También procederá dicho recurso en el caso de falta de respuesta en los plazos a que se refiere el artículo 36 de la ley.

Guatemala

Al igual que en el caso de El Salvador, Guatemala tampoco cuenta con una legislación en materia de protección de datos personales, no obstante, su Ley de Acceso a la Información Pública, contendida en el Decreto N° 57-2008 aborda algunos aspectos relacionados con la protección de datos, en efecto, su artículo 1° dispone que uno de sus propósitos es "Garantizar a toda persona individual el derecho a conocer y proteger loa datos personales de lo que de ella conste en archivos estatales, así como de las actualizaciones de los mismos". Es decir, la señalada ley solo regula el tratamiento de datos personales en entidades públicas.

A continuación, los numerales 1 y 2 del artículo 9, conceptualizan los datos personales y los datos personales sensibles, al señalar que los datos personales son "Los relativos a cualquier información concerniente a personas naturales identificadas o identificables". Y que los datos personales sensibles son "Aquellos datos personales que se refieren a las características físicas o morales de las personas o a hechos o circunstancias de su vida privada o actividad, tales como los hábitos personales, el origen racial, el origen étnico, las ideologías y opiniones políticas, las creencias o convicciones religiosas, los estados de salud físicos o psíquicos, preferencia o vida sexual, situación moral ·y familiar u otras cuestiones intimas de similar naturaleza".

El Capítulo Sexto del Título I sobre disposiciones generales de la ley, regula el "hábeas data", señalando su artículo 30 que los sujetos obligados serán responsables de los datos personales y en relación con estos, deberán: 1. Adoptar los procedimientos adecuados para recibir y

[438] En la actualidad el Instituto de Acceso a la Información Pública – IAIP- salvadoreño solamente tiene competencias para trabajar con los datos que resguardan y tratan las instituciones públicas, por lo que es necesario y pertinente que la legislación actual regule de mejor manera también a las instituciones privadas que manejan datos personales, debiendo revisarse por ejemplo la Ley que norma el funcionamiento de los burós de crédito.

responder las solicitudes de acceso y corrección de datos que sean presentados por los titulares de los mismos o sus representantes legales, así como capacitar a los servidores públicos y dar a conocer información sobre sus políticas en relación con la protección de tales datos; 2. Administrar datos personales solo cuando estos sean adecuados, pertinentes y no excesivos, en relación con los propósitos para los cuales se hayan obtenido; 3. Poner a disposición de la persona individual, a partir del momento en el cual se recaben datos personales, el documento en el que se establezcan los propósitos para su tratamiento; 4. Procurar que los datos personales sean exactos y actualizados; 5. Adoptar las medidas necesarias que garanticen la seguridad, y en su caso confidencia o reserva de los datos personales evitando su alteración, pérdida, transmisión y acceso no autorizado. Los sujetos activos no podrán usar la información obtenida para fines comerciales, salvo autorización expresa del titular de la Información.

El artículo 31 de la ley guatemalteca se refiere al consentimiento expreso de su titular para el tratamiento de datos de carácter personal de parte de los sujetos obligados al señalar que;

> "*Los sujetos obligados no podrán difundir, distribuir o comercializar los datos personales contenidos en los sistemas de información desarrollados en el ejercicio de sus funciones, salvo que hubiere mediado el consentimiento expreso por escrito de los individuos a que hiciere referencia la información. El Estado vigilará que en caso de que se otorgue el consentimiento expreso, no se incurra en ningún momento en vicio de la voluntad en perjuicio del gobernado, explicándole claramente las consecuencias de sus actos. Queda expresamente prohibida la comercialización por cualquier medio de datos sensibles o datos personales sensibles"*.

Según el artículo 32 no se requerirá el consentimiento del titular de la información para proporcionar los datos personales en los siguientes casos: 1. Los necesarios por razones estadísticas, científicas o de interés general previstas en ley, previo procedimiento por el cual no puedan asociarse los datos personales con el individuo a quien se refieran; 2. Cuando se transmitan entre sujetos obligados o entre dependencias y entidades del Estado, siempre y cuando los datos se utilicen para el ejercicio de facultades propias de los mismos; 3. Cuando exista una orden judicial; 4. Los establecidos en esta ley; 5. Los contenidos en los registros públicos; 6. En los demás casos que establezcan las leyes. En ningún caso se podrán crear bancos de datos o archivos con datos sensibles o datos personales sensibles, salvo que sean utilizados para el servicio y atención propia de la institución.

Sobre el tratamiento de los datos personales el artículo 34 dispone que los titulares o sus representantes legales podrán solicitar, previa acreditación, que modifiquen sus datos personales contenidos en cualquier sistema de información. Con tal propósito, el Interesado debe entregar una solicitud de modificaciones, en la que señale el sistema de datos personales, indique las modificaciones que desea realizar y aporte la documentación que motive su petición. El sujeto obligado debe entregar al solicitante, en un plazo no mayor de treinta días hábiles desde la presentación de la solicitud, una resolución que haga constar las modificaciones o bien, le informe de manera fundamentada, las razones por las cuales no procedieron las mismas.

Honduras

En Honduras en la actualidad no existe una ley que regule la protección de datos personales, sin embrago, en el año 2015 se presentó un proyecto de Ley de Protección de Datos Personales. Este proyecto se basó en el anteproyecto que fue presentado por el Instituto Nacional de Acceso

a la Información Pública de ese país en el año 2013, con el apoyo de la Agencia Española de Cooperación Internacional para el Desarrollo (AECID). Actualmente, el proyecto sigue en proceso de tramitación legislativa. A falta de una legislación especial, los datos personales en Honduras cuentan con al menos una protección que se reconoce en la Ley del Instituto de Acceso a la Información Pública, Decreto Legislativo N° 170 – 2006[439], que en el Capítulo V regula la protección de datos y el hábeas data, estableciendo la figura del Comisionado Nacional de Derechos Humanos como una oficina facultada para incoar acciones para la protección de datos personales; además establece una prohibición en la cual ninguna persona puede solicitar a otros datos personales que puedan generar algún tipo de discriminación o poner en riesgo los derechos morales y patrimoniales de ese individuo.

El artículo 25 de la ley dispone la prohibición de entrega de información al señalar que "Ninguna persona podrá obligar a otra a proporcionar datos personales que puedan originar discriminación o causar daños o riesgos patrimoniales o morales de las personas".

México

Como se abordó en líneas anteriores, México reconoce de manera expresa la protección de datos personales como un derecho fundamental en el artículo 16 de la Constitución Política de los Estados Unidos Mexicanos, y además cuenta con una abundante legislación en la materia, tanto a nivel nacional como federal para cada uno de los Estados que conforman la nación. Expresión de aquello es la Ley Federal de Protección de Datos Personales en Posesión de los Particulares - LFPDPPP[440], dirigida a personas físicas o morales de carácter privado, y Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados - LGPDPPSO[441], aplicable para cualquier autoridad de los tres niveles de gobierno, órganos autónomos, partidos políticos, fideicomisos y fondos públicos. A continuación se abordarán los principales contenidos y alcances de ambas legislaciones.

Ley Federal de Protección de Datos Personales en Posesión de los Particulares – LFPDPPP

Constituye un cuerpo normativo aprobado por el Congreso Mexicano el 27 de abril de 2010, que tiene como objetivo regular el derecho a la autodeterminación informativa. La Ley fue publicada el 5 de julio de 2010 en el Diario Oficial de la Federación y entró en vigor el 6 de julio del año 2010. Sus disposiciones son aplicables a todas las personas físicas o morales, del sector privado. Su complemento en la aplicación de sus disposiciones está contenido en el Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, Publicado en el Diario Oficial de La Federación el 21 de diciembre de 2011[442].

---

[439] Ver en: https://portalunico.iaip.gob.hn/assets/docs/leyes/ley-de-transparencia-y-reglamento.pdf consulta realizada el 7 de agosto de 2020.

[440] Ver en: http://www.diputados.gob.mx/LeyesBiblio/pdf/LFPDPPP.pdf consulta realizada el 7 de agosto de 2020.

[441]Ver:http://corpusiurispdp.inai.org.mx/iberoamericano/Instrumentos/LGPDPPSO.pdf#search=ANY%28protecci%C3%B3n%20de%20datos%29 consulta realizada el 7 de agosto de 2020.

[442] Ver en: http://www.diputados.gob.mx/LeyesBiblio/regley/Reg_LFPDPPP.pdf consulta realizada el 8 de agosto de 2020.

La LFPDPPP se estructura en once capítulos, el Capítulo I "Disposiciones Generales", aborda en el artículo 1° el objeto de la ley al señalar que: "La presente Ley es de orden público y de observancia general en toda la República y tiene por objeto la protección de los datos personales en posesión de los particulares, con la finalidad de regular su tratamiento legítimo, controlado e informado, a efecto de garantizar la privacidad y el derecho a la autodeterminación informativa de las personas".

El artículo 2 se refiere a los sujetos que se obligan por sus disposiciones, señalando que son sujetos regulados por esta ley los particulares sean personas físicas o morales de carácter privado que lleven a cabo el tratamiento de datos personales; aborda también qué sujetos se exceptúan de sus preceptos, y que son: Las sociedades de información crediticia en los supuestos de la Ley para Regular las Sociedades de Información Crediticia y demás disposiciones aplicables, y las personas que lleven a cabo la recolección y almacenamiento de datos personales, que sea para uso exclusivamente personal, y sin fines de divulgación o utilización comercial.

Siguiendo la experiencia comparada, el artículo 3 conceptualiza un conjunto de términos, definiendo entre otros a los Datos personales como cualquier información concerniente a una persona física identificada o identificable; y a los Datos personales sensibles, como aquellos datos personales que afectan la esfera más íntima de su titular, o cuya utilización indebida pueda dar origen a discriminación o conlleve un riesgo grave para este. En particular, se consideran sensibles aquellos que puedan revelar aspectos como origen racial o étnico, estado de salud presente y futuro, información genética, creencias religiosas, filosóficas y morales, afiliación sindical, opiniones políticas y preferencia sexual.

El artículo 4 se refiere a los límites, o si se quiere a las hipótesis que exceptúan la aplicación de esta ley, y que son: la protección de la seguridad nacional, el orden, la seguridad y la salud públicos, así como los derechos de terceros.

El Capítulo II se titula "De los Principios de la Protección de Datos Personales", estableciendo el artículo 6 que "Los responsables en el tratamiento de datos personales, deberán observar los principios de licitud, consentimiento, información, calidad, finalidad, lealtad, proporcionalidad y responsabilidad, previstos en la Ley".

Un aspecto novedoso de la ley es que el artículo 8 reconoce la existencia del consentimiento tácito, en efecto, se entenderá que el titular consiente tácitamente el tratamiento de sus datos, cuando habiéndose puesto a su disposición el aviso de privacidad, no manifieste su oposición.

El artículo 9 agrega sobre el consentimiento y los datos sensibles que el responsable[443] deberá obtener el consentimiento expreso y por escrito del titular para su tratamiento, a través de su firma autógrafa, firma electrónica, o cualquier mecanismo de autenticación que al efecto se establezca. No podrán crearse bases de datos que contengan datos personales sensibles, sin que se justifique la creación de estas para finalidades legítimas, concretas y acordes con las actividades o fines explícitos que persigue el sujeto regulado.

No será necesario el consentimiento para el tratamiento de los datos personales cuando: I. Esté previsto en una Ley; II. Los datos figuren en fuentes de acceso público; III. Los datos

[443] El numeral XIV del artículo 3 de la ley señala que el Responsable es la "Persona física o moral de carácter privado que decide sobre el tratamiento de datos personales".

personales se sometan a un procedimiento previo de disociación; IV. Tenga el propósito de cumplir obligaciones derivadas de una relación jurídica entre el titular y el responsable; V. Exista una situación de emergencia que potencialmente pueda dañar a un individuo en su persona o en sus bienes; VI. Sean indispensables para la atención médica, la prevención, diagnóstico, la prestación de asistencia sanitaria, tratamientos médicos o la gestión de servicios sanitarios, mientras el titular no esté en condiciones de otorgar el consentimiento, en los términos que establece la Ley General de Salud y demás disposiciones jurídicas aplicables y que dicho tratamiento de datos se realice por una persona sujeta al secreto profesional u obligación equivalente, o VII. Se dicte resolución de autoridad competente[444].

De conformidad al artículo 19,

> *"Todo responsable que lleve a cabo tratamiento de datos personales deberá establecer y mantener medidas de seguridad administrativas, técnicas y físicas que permitan proteger los datos personales contra daño, pérdida, alteración, destrucción o el uso, acceso o tratamiento no autorizado. Los responsables no adoptarán medidas de seguridad menores a aquellas que mantengan para el manejo de su información. Asimismo, se tomará en cuenta el riesgo existente, las posibles consecuencias para los titulares, la sensibilidad de los datos y el desarrollo tecnológico"*.

Luego, agrega el artículo 20 que:

> *"Las vulneraciones de seguridad ocurridas en cualquier fase del tratamiento que afecten de forma significativa los derechos patrimoniales o morales de los titulares, serán informadas de forma inmediata por el responsable al titular, a fin de que este último pueda tomar las medidas correspondientes a la defensa de sus derechos"*.

Sobre la confidencialidad en el tratamiento de los datos, el artículo 21 dispone que:

> *"El responsable o terceros que intervengan en cualquier fase del tratamiento de datos personales deberán guardar confidencialidad respecto de éstos, obligación que subsistirá aun después de finalizar sus relaciones con el titular o, en su caso, con el responsable"*.

El Capítulo III se titula "De los Derechos de los Titulares de los Datos Personales" reconociendo el artículo 22 que "Cualquier titular, o en su caso su representante legal, podrá ejercer los derechos de acceso, rectificación, cancelación y oposición previstos en la presente Ley. El ejercicio de cualquiera de ellos no es requisito previo ni impide el ejercicio de otro. Los datos personales deben ser resguardados de tal manera que permitan el ejercicio sin dilación de estos derechos".

El Capítulo IV "Del Ejercicio de los Derechos de Acceso, Rectificación, Cancelación y Oposición", donde se aborda que el titular o su representante legal podrán solicitar al responsable en cualquier momento el acceso, rectificación, cancelación u oposición, respecto de los datos personales que le conciernen. Además, la solicitud de acceso, rectificación, cancelación u oposición deberá contener y acompañar: El nombre del titular y domicilio u otro medio para comunicarle la respuesta a su solicitud; Los documentos que acrediten la identidad o, en su caso, la representación legal del titular; La descripción clara y precisa de los datos

[444] Artículo 10 de la Ley.

personales respecto de los que se busca ejercer alguno de los derechos antes mencionados, y cualquier otro elemento o documento que facilite la localización de los datos personales.

En el Capítulo V denominado "De la Transferencia de Datos", se establecen entre otras materias, las excepciones al otorgamiento del consentimiento del titular, para el tratamiento de datos o si se quiere, se dispone en el artículo 37 cuando pueden realizarse transferencias nacionales o internacionales de datos, sin el consentimiento de su titular, y que son a saber: Cuando la transferencia esté prevista en una Ley o Tratado en los que México sea parte; Cuando la transferencia sea necesaria para la prevención o el diagnóstico médico, la prestación de asistencia sanitaria, tratamiento médico o la gestión de servicios sanitarios; Cuando la transferencia sea efectuada a sociedades controladoras, subsidiarias o afiliadas bajo el control común del responsable, o a una sociedad matriz o a cualquier sociedad del mismo grupo del responsable que opere bajo los mismos procesos y políticas internas; Cuando la transferencia sea necesaria por virtud de un contrato celebrado o por celebrar en interés del titular, por el responsable y un tercero; Cuando la transferencia sea necesaria o legalmente exigida para la salvaguarda de un interés público, o para la procuración o administración de justicia; Cuando la transferencia sea precisa para el reconocimiento, ejercicio o defensa de un derecho en un proceso judicial, y cuando la transferencia sea precisa para el mantenimiento o cumplimiento de una relación jurídica entre el responsable y el titular.

El Capítulo VI "De las Autoridades", se refiere a la autoridad de control en materia de protección de datos, que en el caso mexicano es el Instituto Nacional de Transparencia, Acceso a la Información Pública y Protección de Datos Personales y cuyo objeto de conformidad al artículo 38 de la ley será "difundir el conocimiento del derecho a la protección de datos personales en la sociedad mexicana, promover su ejercicio y vigilar por la debida observancia de las disposiciones previstas en la presente Ley y que deriven de la misma; en particular aquellas relacionadas con el cumplimiento de obligaciones por parte de los sujetos regulados por este ordenamiento".

El Capítulo VII se titula "Del Procedimiento de Protección de los Derechos", entre los artículos 45 y 58 regula el procedimiento para que el titular de los datos pueda reclamar o buscar tutela, presentando una solicitud de protección de datos que se formula ante el Instituto Nacional de Transparencia, Acceso a la Información Pública y Protección de Datos Personales, en efecto el titular de los datos o su representante legal, expresando con claridad el contenido de su reclamación y de los preceptos de la ley que se consideran vulnerados. La solicitud de protección de datos deberá presentarse dentro de los quince días siguientes a la fecha en que se comunique la respuesta al titular por parte del responsable. En el caso de que el titular de los datos no reciba respuesta por parte del responsable, la solicitud de protección de datos podrá ser presentada a partir de que haya vencido el plazo de respuesta previsto para el responsable. En este caso, bastará que el titular de los datos acompañe a su solicitud de protección de datos el documento que pruebe la fecha en que presentó la solicitud de acceso, rectificación, cancelación u oposición.

La solicitud de protección de datos también procederá en los mismos términos cuando el responsable no entregue al titular los datos personales solicitados; o lo haga en un formato incomprensible, se niegue a efectuar modificaciones o correcciones a los datos personales, el titular no esté conforme con la información entregada por considerar que es incompleta o no corresponda a la información requerida.

Recibida la solicitud de protección de datos ante el Instituto, se dará traslado de esta al responsable, para que, en el plazo de quince días, emita respuesta, ofrezca las pruebas que estime pertinentes y manifieste por escrito lo que a su derecho convenga. El Instituto admitirá las pruebas que estime pertinentes y procederá a lo que la ley denomina "desahogo". Asimismo, podrá solicitar del responsable las demás pruebas que estime necesarias.

Concluido el desahogo de las pruebas, el Instituto notificará al responsable el derecho que le asiste para que, de considerarlo necesario, presente sus alegatos dentro de los cinco días siguientes a su notificación. Para el debido desahogo del procedimiento, el Instituto resolverá sobre la solicitud de protección de datos formulada, una vez analizadas las pruebas y demás elementos de convicción que estime pertinentes, como pueden serlo aquellos que deriven de la o las audiencias que se celebren con las partes.

Los demás aspectos del procedimiento tales como la forma, términos y plazos conforme a los que se desarrollará la tutela de la protección de derechos, estarán regulados en el respectivo Reglamento[445].

El Capítulo VIII "Del Procedimiento de Verificación", aborda la revisión que hará el Instituto del cumplimiento de la presente ley y de la normatividad que de ésta derive. La verificación podrá iniciarse de oficio o a petición de parte. La verificación de oficio procederá cuando se dé el incumplimiento a resoluciones dictadas con motivo de procedimientos de protección de derechos a que se refiere el procedimiento de protección de datos señalado en el capítulo VII o se presuma fundada y motivadamente la existencia de violaciones a la ley.

El Capítulo IX "Del Procedimiento de Imposición de Sanciones", en los artículos 61 y 62 de la ley, además de las disposiciones del Reglamento de la misma, regula el supuesto de si con motivo del desahogo del procedimiento de protección de derechos o del procedimiento de verificación que realice el Instituto, este tuviera conocimiento de un presunto incumplimiento de alguno de los principios o disposiciones de la ley, iniciando el procedimiento respectivo para determinar la sanción que corresponda. Dichas sanciones derivadas de las infracciones del responsable del tratamiento de datos están reguladas en el Capítulo X de la ley, artículos 63 y 64.

El Capítulo XI, "De los Delitos en Materia del Tratamiento Indebido de Datos Personales", aborda como lo indica su título, las penas derivadas de las conductas delictivas relacionadas con el derecho a la protección de datos. Estableciendo que "se impondrán de tres meses a tres años de prisión al que, estando autorizado para tratar datos personales, con ánimo de lucro, provoque una vulneración de seguridad a las bases de datos bajo su custodia" (artículo 67). "Así como se sancionará con prisión de seis meses a cinco años al que, con el fin de alcanzar un lucro indebido, trate datos personales mediante el engaño, aprovechándose del error en que se encuentre el titular o la persona autorizada para transmitirlos" (artículo 68).

[445] Ver en: http://www.diputados.gob.mx/LeyesBiblio/regley/Reg_LFPDPPP.pdf consulta realizada el 8 de agosto de 2020.

Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados – LGPDPPSO[446]

Esta ley se publica en el Diario Oficial de la Federación el 26 de enero de 2017, y como se observa de su revisión, regula en detalle la protección de datos, recogiendo en parte el desarrollo que esta materia ha tenido principalmente en el ámbito europeo, estando su articulado y contenido influenciado por el Reglamento Europeo de Protección de Datos Personales 2016/679.

La LGPDPPSO se estructura en once títulos, cada uno con sus respectivos capítulos, con un total de 168 artículos y 8 artículos transitorios. El Titulo Primero "Disposiciones Generales", consta de dos capítulos, el Capítulo I se refiere al objeto de la ley, disponiendo los incisos 4° y 5° de su artículo primero que "Tiene por objeto establecer las bases, principios y procedimientos para garantizar el derecho que tiene toda persona a la protección de sus datos personales, en posesión de sujetos obligados.

Son sujetos obligados por esta Ley, en el ámbito federal, estatal y municipal, cualquier autoridad, entidad, órgano y organismo de los Poderes Ejecutivo, Legislativo y Judicial, órganos autónomos, partidos políticos, fideicomisos y fondos públicos.

El artículo 3°, en treintaicuatro numerales, conceptualiza diversos términos tales como Datos personales al señalar que son "cualquier información concerniente a una persona física identificada o identificable. Se considera que una persona es identificable cuando su identidad pueda determinarse directa o indirectamente a través de cualquier información"; y Datos personales sensibles, definiéndolos como "Aquellos que se refieran a la esfera más íntima de su titular, o cuya utilización indebida pueda dar origen a discriminación o conlleve un riesgo grave para éste. De manera enunciativa más no limitativa, se consideran sensibles los datos personales que puedan revelar aspectos como origen racial o étnico, estado de salud presente o futuro, información genética, creencias religiosas, filosóficas y morales, opiniones políticas y preferencia sexual".

Su artículo 4°, además, dispone que la ley será aplicable a cualquier tratamiento de datos personales que obren en soportes físicos o electrónicos, con independencia de la forma o modalidad de su creación, tipo de soporte, procesamiento, almacenamiento y organización.

También su artículo 8 señala expresamente cuáles son los criterios de aplicación y hermenéuticos sobre las disposiciones de la ley, al señalar que su aplicación e interpretación se realizará conforme a lo dispuesto en la Constitución Política de los Estados Unidos Mexicanos, los Tratados Internacionales de los que el Estado mexicano sea parte, así como las resoluciones y sentencias vinculantes que emitan los órganos nacionales e internacionales especializados, favoreciendo en todo tiempo el derecho a la privacidad, la protección de datos personales y la más amplia protección a las personas. Para el caso de la interpretación, se podrán tomar en cuenta los criterios, determinaciones y opiniones de los organismos nacionales e internacionales, en materia de protección de datos personales.

El Capítulo II del Título Primero "Del Sistema Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales", integrado por la Ley General de Transparencia

[446]Ver:http://corpusiurispdp.inai.org.mx/iberoamericano/Instrumentos/LGPDPPSO.pdf#search=ANY%28protecci%C3%B3n%20de%20datos%29 consulta realizada el 8 de agosto de 2020.

y Acceso a la Información Pública, y que en materia de protección de datos personales, tiene como función coordinar y evaluar las acciones relativas a la política pública transversal de protección de datos personales, así como establecer e implementar criterios y lineamientos en la materia, de conformidad con lo señalado en la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados y la Ley General de Transparencia y Acceso a la Información Pública y demás normatividad aplicable.

El Título Segundo "Principios y Deberes", consta también de dos capítulos, el Capítulo I "De los Principios" y el Capítulo II "De los Deberes". El artículo 16 dispone que el responsable deberá observar los principios de licitud, finalidad, lealtad, consentimiento, calidad, proporcionalidad, información y responsabilidad en el tratamiento de datos personales.

Luego, el artículo 20 establece que cuando no se actualicen algunas de las causales de excepción previstas en el artículo 22 de la presente Ley, el responsable deberá contar con el consentimiento previo del titular para el tratamiento de los datos personales, el cual deberá otorgarse de forma: I. Libre: Sin que medie error, mala fe, violencia o dolo que puedan afectar la manifestación de voluntad del titular; II. Específica: Referida a finalidades concretas, lícitas, explícitas y legítimas que justifiquen el tratamiento; y III. Informada: Que el titular tenga conocimiento del aviso de privacidad previo al tratamiento a que serán sometidos sus datos personales.

Y, al igual que la LFPDPPP, esta ley establece la posibilidad de que el consentimiento sea expreso y también tácito. En efecto el artículo 21 dispone;

> *"El consentimiento podrá manifestarse de forma expresa o tácita. Se deberá entender que el consentimiento es expreso cuando la voluntad del titular se manifieste verbalmente, por escrito, por medios electrónicos, ópticos, signos inequívocos o por cualquier otra tecnología. El consentimiento será tácito cuando habiéndose puesto a disposición del titular el aviso de privacidad, éste no manifieste su voluntad en sentido contrario. Por regla general será válido el consentimiento tácito, salvo que la ley o las disposiciones aplicables exijan que la voluntad del titular se manifieste expresamente. Tratándose de datos personales sensibles el responsable deberá obtener el consentimiento expreso y por escrito del titular para su tratamiento, a través de su firma autógrafa, firma electrónica o cualquier mecanismo de autenticación que al efecto se establezca, salvo en los casos previstos en el artículo 22 de esta Ley".*
>
> *"Artículo 22; El responsable no estará obligado a recabar el consentimiento del titular para el tratamiento de sus datos personales en los siguientes casos: I. Cuando una ley así lo disponga, debiendo dichos supuestos ser acordes con las bases, principios y disposiciones establecidos en esta Ley, en ningún caso, podrán contravenirla; II. Cuando las transferencias que se realicen entre responsables sean sobre datos personales que se utilicen para el ejercicio de facultades propias, compatibles o análogas con la finalidad que motivó el tratamiento de los datos personales; III. Cuando exista una orden judicial, resolución o mandato fundado y motivado de autoridad competente; IV. Para el reconocimiento o defensa de derechos del titular ante autoridad competente; V. Cuando los datos personales se requieran para ejercer un derecho o cumplir obligaciones derivadas de una relación jurídica entre el titular y el responsable; VI. Cuando exista una situación de emergencia que potencialmente pueda dañar a un individuo en su persona o en sus bienes; VII. Cuando los datos*

> *personales sean necesarios para efectuar un tratamiento para la prevención, diagnóstico, la prestación de asistencia sanitaria; VIII. Cuando los datos personales figuren en fuentes de acceso público; IX. Cuando los datos personales se sometan a un procedimiento previo de disociación, o X. Cuando el titular de los datos personales sea una persona reportada como desaparecida en los términos de la ley en la materia".*

En relación a los deberes, que se consagran como las medidas de seguridad que debe adoptar el responsable del tratamiento de los datos, el artículo 31 dispone que "el responsable deberá establecer y mantener las medidas de seguridad de carácter administrativo, físico y técnico para la protección de los datos personales, que permitan protegerlos contra daño, pérdida, alteración, destrucción o su uso, acceso o tratamiento no autorizado, así como garantizar su confidencialidad, integridad y disponibilidad".

El Título Tercero, "Derechos de los Titulares y su Ejercicio" se configura por tres capítulos, el Capítulo I "De los Derechos de Acceso, Rectificación, Cancelación y Oposición", así el artículo 43 reconoce los denominados "derechos arco", a los que la propia ley en su artículo 3° numeral XI hace referencia. Dispone el citado artículo 43;

> *"En todo momento el titular o su representante podrán solicitar al responsable, el acceso, rectificación, cancelación u oposición al tratamiento de los datos personales que le conciernen, de conformidad con lo establecido en el presente Título. El ejercicio de cualquiera de los derechos ARCO no es requisito previo, ni impide el ejercicio de otro".*

El Capítulo II "Del Ejercicio de los Derechos de Acceso, Rectificación, Cancelación y Oposición", este capítulo regula el ejercicio de los derechos ARCO, para lo que será necesario acreditar la identidad del titular y, en su caso, la identidad y personalidad con la que actúe el representante. El ejercicio de los derechos ARCO por persona distinta a su titular o a su representante, será posible, excepcionalmente, en aquellos supuestos previstos por disposición legal, o en su caso, por mandato judicial.

El ejercicio de los derechos ARCO deberá ser gratuito y solo podrán realizarse cobros para recuperar los costos de reproducción, certificación o envío, conforme a la normatividad que resulte aplicable. Para efectos de acceso a datos personales, las leyes que establezcan los costos de reproducción y certificación deberán considerar en su determinación que los montos permitan o faciliten el ejercicio de este derecho. Cuando el titular proporcione el medio magnético, electrónico o el mecanismo necesario para reproducir los datos personales, los mismos deberán ser entregados sin costo a este. La información deberá ser entregada sin costo, cuando implique la entrega de no más de veinte hojas simples. Las unidades de transparencia podrán exceptuar el pago de reproducción y envío atendiendo a las circunstancias socioeconómicas del titular. El responsable no podrá establecer para la presentación de las solicitudes del ejercicio de los derechos ARCO algún servicio o medio que implique un costo al titular.

Finalmente, el Capítulo III de este Título, "De la Portabilidad de los Datos", en el artículo 57, dispone:

> *"Cuando se traten datos personales por vía electrónica en un formato estructurado y comúnmente utilizado, el titular tendrá derecho a obtener del responsable una copia de los datos objeto de tratamiento en un formato electrónico estructurado y comúnmente utilizado que le permita seguir utilizándolos. Cuando el titular haya*

> *facilitado los datos personales y el tratamiento se base en el consentimiento o en un contrato, tendrá derecho a transmitir dichos datos personales y cualquier otra información que haya facilitado y que se conserve en un sistema de tratamiento automatizado a otro sistema en un formato electrónico comúnmente utilizado, sin impedimentos por parte del responsable del tratamiento de quien se retiren los datos personales. El Sistema Nacional establecerá mediante lineamientos los parámetros a considerar para determinar los supuestos en los que se está en presencia de un formato estructurado y comúnmente utilizado, así como las normas técnicas, modalidades y procedimientos para la transferencia de datos personales"*.

El Titulo Cuarto "Relación del Responsable[447] y del Encargado[448]", consta de un capítulo único que regula precisamente al Responsable y al Encargado del tratamiento de datos de carácter personal, estableciendo el inciso primero del artículo 59 como criterio general que "La relación entre el responsable y el encargado deberá estar formalizada mediante contrato o cualquier otro instrumento jurídico que decida el responsable, de conformidad con la normativa que le resulte aplicable, y que permita acreditar su existencia, alcance y contenido".

El Titulo Quinto "Comunicaciones de Datos Personales", a través de un único capítulo aborda las transferencias y remisiones de datos personales. Sobre lo cual dispone el artículo 66, inciso primero que:

> *"Toda transferencia deberá formalizarse mediante la suscripción de cláusulas contractuales, convenios de colaboración o cualquier otro instrumento jurídico, de conformidad con la normatividad que le resulte aplicable al responsable, que permita demostrar el alcance del tratamiento de los datos personales, así como las obligaciones y responsabilidades asumidas por las partes"*.

Asimismo, el artículo 71 señala que:

> *"Las remisiones nacionales e internacionales de datos personales que se realicen entre responsable y encargado no requerirán ser informadas al titular, ni contar con su consentimiento"*.

El Titulo Sexto "Acciones Preventivas en Materia de Protección de Datos Personales", se estructura en dos capítulos. El Capítulo I "De las Mejores Prácticas" y el Capítulo II "De las Bases de Datos en Posesión de Instancias de Seguridad, Procuración y Administración de Justicia".

Sobre las mejores prácticas el artículo 72 dispone que, para el cumplimiento de las obligaciones previstas en la ley, el responsable podrá desarrollar o adoptar, en lo individual o en acuerdo con otros responsables, encargados u organizaciones, esquemas de mejores prácticas que tengan por objeto: I. Elevar el nivel de protección de los datos personales; II. Armonizar el tratamiento de datos personales en un sector específico; III. Facilitar el ejercicio de los derechos ARCO por parte de los titulares; IV. Facilitar las transferencias de datos personales;

---

[447] Según el artículo 3° XXVIII de la propia ley, el Responsable se conceptualiza como: "Los sujetos obligados a que se refiere el artículo 1 de la presente Ley que deciden sobre el tratamiento de datos personales".

[448] Según el artículo 3° XV de la propia ley, el Encargado es "La persona física o jurídica, pública o privada, ajena a la organización del responsable, que sola o conjuntamente con otras trate datos personales a nombre y por cuenta del responsable".

V. Complementar las disposiciones previstas en la normatividad que resulte aplicable en materia de protección de datos personales, y VI. Demostrar ante el Instituto o, en su caso, los Organismos garantes, el cumplimiento de la normatividad que resulte aplicable en materia de protección de datos personales.

Con relación a las bases de datos en posesión de instancias de seguridad, procuración y administración de justicia, se desprende del artículo 80 que está limitada a aquellos supuestos y categorías de datos que resulten necesarios y proporcionales para el ejercicio de las funciones en materia de seguridad nacional, seguridad pública, o para la prevención o persecución de los delitos. Deberán ser almacenados en las bases de datos establecidas para tal efecto. Las autoridades que accedan y almacenen los datos personales que se recaben por los particulares en cumplimiento de las disposiciones legales correspondientes, deberán cumplir con las disposiciones señaladas en ley.

El Titulo Séptimo se refiere a los "Responsables en Materia de Protección de Datos Personales en Posesión de los Sujetos Obligados" y consta de dos capítulos: el Capítulo I "Comité de Transparencia" y Capítulo II "Unidad de Transparencia". El artículo 83 dispone que cada responsable contará con un Comité de Transparencia, que se integrará y funcionará conforme a lo dispuesto en la Ley General de Transparencia y Acceso a la Información Pública - LGTAIP, que se publicó en el Diario Oficial de la Federación el 9 de mayo del año 2016. La LGTAIP establece en su artículo 64 que en cada sujeto obligado se integrará un Comité de Transparencia colegiado e integrado por un número impar, designado por el titular u órgano colegiado supremo, según se trate.

El Comité de Transparencia adoptará sus resoluciones por mayoría de votos. En caso de empate, el Presidente tendrá voto de calidad, es decir de desempate. A sus sesiones podrán asistir como invitados aquellos que sus integrantes consideren necesarios, quienes tendrán voz, pero no voto.

Los integrantes del Comité de Transparencia no podrán depender jerárquicamente entre sí, tampoco podrán reunirse dos o más de estos integrantes en una sola persona. Cuando se presente el caso, el titular del sujeto obligado tendrá que nombrar a la persona que supla al subordinado. Los miembros propietarios de los Comités de Transparencia contarán con los suplentes designados de conformidad con la normatividad interna de los respectivos sujetos obligados, y deberán corresponder a personas que ocupen cargos de la jerarquía inmediata inferior a la de dichos propietarios.

En el caso de la Administración Pública Federal, los Comités de las dependencias y entidades se integrarán de la siguiente forma: I. El responsable del área coordinadora de archivos o equivalente; II. El titular de la Unidad de Transparencia, y III. El titular del Órgano Interno de Control de cada dependencia o entidad.

Los integrantes del Comité de Transparencia tendrán acceso a la información para determinar su clasificación, conforme a la normatividad previamente establecida por los sujetos obligados para el resguardo o salvaguarda de la información.

El Centro de Investigación y Seguridad Nacional; el Centro Nacional de Planeación, Análisis e Información para el Combate a la Delincuencia; el Centro Federal de Protección a Personas; las Divisiones de Inteligencia e Investigación de la Policía Federal; la Subprocuraduría Especializada en Investigación de Delincuencia Organizada; la Unidad de Inteligencia Financiera; el Estado Mayor Presidencial, el Estado Mayor de la Defensa Nacional, el Estado

Mayor General de la Armada, la Autoridad Investigadora de la Comisión Federal de Competencia Económica y la del Instituto Federal de Telecomunicaciones o bien, las unidades administrativas que los sustituyan, no estarán sujetos a la autoridad de los Comités de Transparencia a que se refiere el presente artículo, siendo sus funciones responsabilidad exclusiva del titular de la propia entidad o unidad administrativa.

La clasificación, desclasificación y acceso a la información que generen o custodien las instancias de inteligencia e investigación deberá apegarse a los términos previstos en la ley General, a la normativa respectiva y a los protocolos de seguridad y resguardo establecidos para ello.

Además, la LGTAIP precisa quienes son los sujetos obligados, al señalar en su artículo 1° que: "cualquier autoridad, entidad, órgano y organismo de los poderes Legislativo, Ejecutivo y Judicial, órganos autónomos, partidos políticos, fideicomisos y fondos públicos, así como de cualquier persona física, moral o sindicato que reciba y ejerza recursos públicos federales o realice actos de autoridad, en los términos previstos por la Constitución Política de los Estados Unidos Mexicanos y la Ley General de Transparencia y Acceso a la Información Pública".

Por su parte el artículo 85 dispone que cada responsable cuente con una Unidad de Transparencia, que se integrará y funcionará conforme a lo dispuesto en la Ley General de Transparencia y Acceso a la Información Pública.

> *El Artículo 61 de la LGTAIP dispone que; "Los sujetos obligados designarán al responsable de la Unidad de Transparencia que tendrá las siguientes funciones: I. Coordinar la difusión de la información a que se refiere el Capítulo I del Título Tercero de esta Ley, así como los Capítulos II a V del Título Quinto de la Ley General, según corresponda, y propiciar que las Áreas la actualicen periódicamente; II. Recibir y dar trámite a las solicitudes de acceso a la información; III. Auxiliar a los particulares en la elaboración de solicitudes de acceso a la información y, en su caso, orientarlos sobre los sujetos obligados competentes conforme a la normatividad aplicable; IV. Realizar los trámites internos necesarios para la atención de las solicitudes de acceso a la información; V. Efectuar las notificaciones a los solicitantes; VI. Proponer al Comité de Transparencia los procedimientos internos que aseguren la mayor eficiencia en la gestión de las solicitudes de acceso a la información conforme a la normatividad aplicable; VII. Proponer personal habilitado que sea necesario para recibir y dar trámite a las solicitudes de acceso a la información; VIII. Llevar un registro de las solicitudes de acceso a la información, respuestas, resultados, costos de reproducción y envío; IX. Promover e implementar políticas de transparencia proactiva procurando su accesibilidad; X. Fomentar la transparencia al interior del sujeto obligado; XI. Hacer del conocimiento de la instancia competente la probable responsabilidad por el incumplimiento de las obligaciones previstas en la presente Ley y en las demás disposiciones aplicables, y XII. Las que se desprendan de la Ley General y demás normatividad aplicable necesarias para garantizar el ejercicio del derecho de acceso a la información entre el sujeto obligado y los solicitantes.*
> *Los sujetos obligados promoverán acuerdos con instituciones públicas especializadas que pudieran auxiliarles a entregar las respuestas a solicitudes de información, en la lengua indígena, braille o cualquier formato accesible correspondiente, en forma más eficiente".*

Además, agrega que los responsables que en el ejercicio de sus funciones sustantivas lleven a cabo tratamientos de datos personales relevantes o intensivos, podrán designar a un oficial de protección de datos personales especializado en la materia, quien realizará las atribuciones mencionadas y formará parte de la Unidad de Transparencia.

El Título Octavo "Organismos Garantes", se estructura sobre tres capítulos. El Capítulo I "Del Instituto de Transparencia, Acceso a la Información y Protección de Datos Personales", al que se refiere el artículo 88 en cuanto a que su integración, procedimiento de designación de sus integrantes y funcionamiento del mismo, así como del Consejo Consultivo se regulará por lo dispuesto por la Ley General de Transparencia y Acceso a la Información Pública, que señala en el inciso 1° de su artículo 17 que "El Instituto es un organismo autónomo, especializado, independiente, imparcial y colegiado, con personalidad jurídica y patrimonio propio, con plena autonomía técnica, de gestión, capacidad para decidir sobre el ejercicio de su presupuesto y determinar su organización interna, responsable de garantizar en el ámbito federal, el ejercicio de los derechos de acceso a la información y la protección de datos personales, conforme a los principios y bases establecidos por el artículo 60 de la Constitución, la Ley General, así como por lo previsto en esta Ley y demás disposiciones aplicables". Luego el artículo 89 LGPDPSO, establece las funciones que se le asignan al Instituto en materia de protección de datos.

El Capítulo II "De los Organismos Garantes", aborda en los artículos 90 y 91 su integración y atribuciones respectivamente.

El Capítulo III "De la Coordinación y Promoción del Derecho a la Protección de Datos Personales", que en el artículo 92 dispone que "Los responsables deberán colaborar con el Instituto y los organismos garantes, según corresponda, para capacitar y actualizar de forma permanente a todos sus servidores públicos en materia de protección de datos personales, a través de la impartición de cursos, seminarios, talleres y cualquier otra forma de enseñanza y entrenamiento que se considere pertinente".

El Titulo Noveno "De los Procedimientos de Impugnación en Materia de Protección de Datos Personales en Posesión de Sujetos Obligados", se estructura sobre seis capítulos. El Capítulo I "Disposiciones Comunes los Recursos de Revisión y Recursos de Inconformidad"; el Capítulo II "Del Recurso de Revisión ante el Instituto y los Organismos Garantes"; el Capítulo III "Del Recurso de Inconformidad ante el Instituto"; el Capítulo IV "De la Atracción de los Recursos de Revisión"; el Capítulo V "Del Recurso de Revisión en Materia de Seguridad Nacional" y el Capítulo VI "De los Criterios de Interpretación".

A continuación, el Título X se refiere a la "Facultad de Verificación del Instituto y los Organismos Garantes", que tiene un único capítulo que se refiere al "Procedimiento de Verificación", que en su artículo 146 dispone que "El Instituto y los Organismos garantes, en el ámbito de sus respectivas competencias, tendrán la atribución de vigilar y verificar el cumplimiento de las disposiciones contenidas en la presente Ley y demás ordenamientos que se deriven de ésta. En el ejercicio de las funciones de vigilancia y verificación, el personal del Instituto o, en su caso, de los Organismos garantes estarán obligados a guardar confidencialidad sobre la información a la que tengan acceso en virtud de la verificación correspondiente. El responsable no podrá negar el acceso a la documentación solicitada con motivo de una verificación, o a sus bases de datos personales, ni podrá invocar la reserva o la confidencialidad de la información".

Finalmente, el Título XI sobre "Medidas de Apremio y Responsabilidades", se conforma por dos capítulos, el Capítulo I "De las Medidas de Apremio", a las que se refiere el artículo 153, al señalar que "El Instituto y los Organismos garantes podrán imponer las siguientes medidas de apremio para asegurar el cumplimiento de sus determinaciones: I. La amonestación pública, o II. La multa. El incumplimiento de los sujetos obligados será difundido en los portales de obligaciones de transparencia del Instituto y los Organismos garantes y considerados en las evaluaciones que realicen éstos. En caso de que el incumplimiento de las determinaciones del Instituto y los Organismos garantes implique la presunta comisión de un delito o una de las conductas señaladas en el artículo 163 de la presente Ley, deberán denunciar los hechos ante la autoridad competente. Las medidas de apremio de carácter económico no podrán ser cubiertas con recursos públicos".

Precisamente en el Capítulo II "De las Sanciones", el señalado artículo 163 dispone que "Serán causas de sanción por incumplimiento de las obligaciones establecidas en la materia de la presente Ley, las siguientes: I. Actuar con negligencia, dolo o mala fe durante la sustanciación de las solicitudes para el ejercicio de los derechos ARCO; II. Incumplir los plazos de atención previstos en la presente Ley para responder las solicitudes para el ejercicio de los derechos ARCO o para hacer efectivo el derecho de que se trate; III. Usar, sustraer, divulgar, ocultar, alterar, mutilar, destruir o inutilizar, total o parcialmente y de manera indebida datos personales, que se encuentren bajo su custodia o a los cuales tengan acceso o conocimiento con motivo de su empleo, cargo o comisión; IV. Dar tratamiento, de manera intencional, a los datos personales en contravención a los principios y deberes establecidos en la presente Ley; No contar con el aviso de privacidad, o bien, omitir en el mismo alguno de los elementos a que refiere el artículo 27 de la presente Ley, según sea el caso, y demás disposiciones que resulten aplicables en la materia;

> *"Artículo 27; : El aviso de privacidad a que se refiere el artículo 3, fracción II, se pondrá a disposición del titular en dos modalidades: simplificado e integral. El aviso simplificado deberá contener la siguiente información: I. La denominación del responsable; II. Las finalidades del tratamiento para las cuales se obtienen los datos personales, distinguiendo aquéllas que requieran el consentimiento del titular; III. Cuando se realicen transferencias de datos personales que requieran consentimiento, se deberá informar: a) Las autoridades, poderes, entidades, órganos y organismos gubernamentales de los tres órdenes de gobierno y las personas físicas o morales a las que se transfieren los datos personales, y b) Las finalidades de estas transferencias; IV. Los mecanismos y medios disponibles para que el titular, en su caso, pueda manifestar su negativa para el tratamiento de sus datos personales para finalidades y transferencias de datos personales que requieren el consentimiento del titular, y V. El sitio donde se podrá consultar el aviso de privacidad integral. La puesta a disposición del aviso de privacidad al que refiere este artículo no exime al responsable de su obligación de proveer los mecanismos para que el titular pueda conocer el contenido del aviso de privacidad al que se refiere el artículo siguiente. Los mecanismos y medios a los que se refiere la fracción IV de este artículo, deberán estar disponibles para que el titular pueda manifestar su negativa al tratamiento de sus datos personales para las finalidades o transferencias que requieran el consentimiento del titular, previo a que ocurra dicho tratamiento".*

VI. Clasificar como confidencial, con dolo o negligencia, datos personales sin que se cumplan las características señaladas en las leyes que resulten aplicables. La sanción sólo procederá cuando exista una resolución previa, que haya quedado firme, respecto del criterio de clasificación de los datos personales; VII. Incumplir el deber de confidencialidad establecido en el artículo 42 de la presente Ley; VIII. No establecer las medidas de seguridad en los términos que establecen los artículos 31, 32 y 33 de la presente Ley;

> *"Artículo 31. Con independencia del tipo de sistema en el que se encuentren los datos personales o el tipo de tratamiento que se efectúe, el responsable deberá establecer y mantener las medidas de seguridad de carácter administrativo, físico y técnico para la protección de los datos personales, que permitan protegerlos contra daño, pérdida, alteración, destrucción o su uso, acceso o tratamiento no autorizado, así como garantizar su confidencialidad, integridad y disponibilidad.*
>
> *"Artículo 32. Las medidas de seguridad adoptadas por el responsable deberán considerar: I. El riesgo inherente a los datos personales tratados; II. La sensibilidad de los datos personales tratados; III. El desarrollo tecnológico; IV. Las posibles consecuencias de una vulneración para los titulares; V. Las transferencias de datos personales que se realicen; VI. El número de titulares; VII. Las vulneraciones previas ocurridas en los sistemas de tratamiento, y VIII. El riesgo por el valor potencial cuantitativo o cualitativo que pudieran tener los datos personales tratados para una tercera persona no autorizada para su posesión".*
>
> "*Artículo 33. Para establecer y mantener las medidas de seguridad para la protección de los datos personales, el responsable deberá realizar, al menos, las siguientes actividades interrelacionadas: I. Crear políticas internas para la gestión y tratamiento de los datos personales, que tomen en cuenta el contexto en el que ocurren los tratamientos y el ciclo de vida de los datos personales, es decir, su obtención, uso y posterior supresión; II. Definir las funciones y obligaciones del personal involucrado en el tratamiento de datos personales; III. Elaborar un inventario de datos personales y de los sistemas de tratamiento; IV. Realizar un análisis de riesgo de los datos personales, considerando las amenazas y vulnerabilidades existentes para los datos personales y los recursos involucrados en su tratamiento, como pueden ser, de manera enunciativa más no limitativa, hardware, software, personal del responsable, entre otros; V. Realizar un análisis de brecha, comparando las medidas de seguridad existentes contra las faltantes en la organización del responsable; VI. Elaborar un plan de trabajo para la implementación de las medidas de seguridad faltantes, así como las medidas para el cumplimiento cotidiano de las políticas de gestión y tratamiento de los datos personales; VII. Monitorear y revisar de manera periódica las medidas de seguridad implementadas, así como las amenazas y vulneraciones a las que están sujetos los datos personales, y VIII. Diseñar y aplicar diferentes niveles de capacitación del personal bajo su mando, dependiendo de sus roles y responsabilidades respecto del tratamiento de los datos personales".*

IX. Presentar vulneraciones a los datos personales por la falta de implementación de medidas de seguridad según los artículos 31, 32 y 33 de la presente Ley; X. Llevar a cabo la transferencia de datos personales, en contravención a lo previsto en la presente Ley; XI.

Obstruir los actos de verificación de la autoridad; XII. Crear bases de datos personales en contravención a lo dispuesto por el artículo 5 de la presente Ley;

> *"Artículo 5. Para los efectos de la presente Ley, se considerarán como fuentes de acceso público: I. Las páginas de Internet o medios remotos o locales de comunicación electrónica, óptica y de otra tecnología, siempre que el sitio donde se encuentren los datos personales esté concebido para facilitar información al público y esté abierto a la consulta general; II. Los directorios telefónicos en términos de la normativa específica; III. Los diarios, gacetas o boletines oficiales, de acuerdo con su normativa; IV. Los medios de comunicación social, y V. Los registros públicos conforme a las disposiciones que les resulten aplicables. Para que los supuestos enumerados en el presente artículo sean considerados fuentes de acceso público será necesario que su consulta pueda ser realizada por cualquier persona no impedida por una norma limitativa, o sin más exigencia que, en su caso, el pago de una contra prestación, derecho o tarifa. No se considerará una fuente de acceso público cuando la información contenida en la misma sea o tenga una procedencia ilícita".*

XIII. No acatar las resoluciones emitidas por el Instituto y los Organismos garantes, y XIV. Omitir la entrega del informe anual y demás informes a que se refiere el artículo 44, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública, o bien, entregar el mismo de manera extemporánea. Las causas de responsabilidad previstas en las fracciones I, II, IV, VI, X, XII, y XIV, así como la reincidencia en las conductas previstas en el resto de las fracciones de este artículo, serán consideradas como graves para efectos de su sanción administrativa. En caso de que la presunta infracción hubiere sido cometida por algún integrante de un partido político, la investigación y, en su caso, sanción, corresponderán a la autoridad electoral competente. Las sanciones de carácter económico no podrán ser cubiertas con recursos públicos".

Como se puede apreciar, el ordenamiento jurídico mexicano cuenta con una robusta legislación en materia de protección de datos de carácter personal, que se entremezcla con las disposiciones de transparencia y acceso a la información pública, y que distingue tanto una regulación para las entidades privadas que realizan tratamiento de datos, como para los organismos públicos que denomina sujetos obligados; esta última legislación, para los sujetos obligados, se encuentra fuertemente influenciada por el RGPD de la UE del año 2016, influjo que se expresa por ejemplo en los Principios que se establecen para regular el tratamiento de datos personales, en los contenidos de los términos que se definen, como es el caso de los denominados datos sensibles, así como en el establecimiento del derecho a la portabilidad de los datos, entre otras cuestiones.

Nicaragua

Además del marco constitucional señalado en líneas anteriores, Nicaragua regula la protección de datos a través de la Ley de Protección de Datos Personales N° 787, aprobada el 21 de Marzo del 2012 y publicada en La Gaceta N° 61 del 29 de Marzo del 2012, la que se ordena en 56 artículos estructurados en nueve capítulos, regulación que se complementa con el respectivo reglamento contenido en el Decreto N° 36-2012, el que a su vez se estructura en 63 artículos contenidos en nueve capítulos. El objeto de la señalada ley es la protección de la persona natural o jurídica frente al tratamiento, automatizado o no, de sus datos personales en ficheros de datos públicos y privados (ámbito de aplicación), a efecto de garantizar el derecho a la

privacidad personal y familiar y el derecho a la autodeterminación informativa (artículos 1° y 2°).

El Capítulo I se titula "Definiciones generales", en su artículo 3° se definen diversos términos entre los que destacan en la letra a) la Autodeterminación Informativa, que "Es el derecho que tiene toda persona a saber quién, cuándo, con qué fines y en qué circunstancias toman contacto con sus datos personales"; la letra d) se refiere al Consentimiento del titular, señalando que "Es toda manifestación de voluntad, libre, inequívoca, específica e informada, mediante la cual el titular de los datos consiente el tratamiento de sus datos personales"; la letra e) aborda los Datos personales, definiéndolos como "toda la información sobre una persona natural o jurídica que la identifica o la hace identificable"; la letra f) define los Datos personales informáticos, señalando que "Son los datos personales tratados a través de medios electrónicos o automatizados"; y la letra g) conceptualiza los Datos personales sensibles, como "toda información que revele el origen racial, étnico, filiación política, credo religioso, filosófico o moral, sindical, relativo a su salud o vida sexual, antecedentes penales o faltas administrativas, económicos financieros; así como información crediticia y financiera y cualquier otra información que pueda ser motivo de discriminación".

El artículo 4° se refiere a la creación de ficheros de datos personales, la que será lícita cuando los datos se encuentren debidamente autorizados y registrados, mediante consentimiento del titular, salvo excepciones de ley. Agrega que los ficheros de datos no pueden tener fines distintos a los permitidos en la ley.

El artículo 5° aborda los requisitos para la obtención de datos personales, señalando que son aquellos: a) Que sean adecuados, proporcionales y necesarios en relación con el ámbito y fin para el que se colectan; y b) Que se haga por medios lícitos que garanticen el derecho de toda persona a la autodeterminación informativa.

A continuación el artículo 6° aborda el consentimiento del titular de los datos, así como las excepciones al mismo, en el sentido de que no será necesario el consentimiento para el tratamiento de datos personales cuando: a) Exista orden motivada, dictada por autoridad judicial competente; b) Los datos personales se sometan a un procedimiento previo de disociación; c) Tenga el propósito de cumplir obligaciones derivadas de una relación jurídica entre el titular y el responsable; y d) Los datos se obtengan de fuentes de acceso público irrestricto y se trate de listados cuyos datos se limiten a nombre, documento nacional de identidad, y fecha de nacimiento.

El Capítulo II se titula "De los responsables de los ficheros de datos", en el artículo 7° se establece el deber de información que tiene el responsable de los ficheros para con los titulares de los datos. El artículo 8° dispone las distintas categorías de los datos personales, distinguiendo entre: Datos personales sensibles, los datos personales relativos a la salud, datos personales informáticos y datos personales comerciales. Reafirmando en su inciso final que "Todos los datos personales sólo podrán ser revelados por consentimiento del Titular de los datos, por ley expresa de interés social o por mandato judicial".

El artículo 10, regula el derecho al olvido digital, estableciendo que el titular de los datos tiene derecho a solicitar a las redes sociales, navegadores y servidores que se supriman y cancelen los datos personales que se encuentren en sus ficheros. En los casos de ficheros de datos de instituciones públicas y privadas que ofrecen bienes y servicios y que por razones contractuales recopilan datos personales, la ley dispone que, una vez terminada la relación contractual, el

titular de estos puede solicitar que se suprima y cancele toda la información personal que se registró mientras era usuario de un servicio o comprador de un bien.

El artículo 12, aborda la confidencialidad en el tratamiento de los datos, al disponer que el responsable del fichero de datos y las personas que intervengan en cualquier fase del tratamiento de datos personales están obligados al secreto profesional respecto de estos. Tal obligación subsistirá aun después de finalizada su relación con el responsable del fichero de datos.

El artículo 14 regula las prohibiciones y excepciones de cesión y transferencia de datos con países u organismos internacionales, que no proporcionen niveles de seguridad y protección adecuados. A continuación, el artículo 15 establece un procedimiento para la cesión y transferencia de datos, describiendo las siguientes fases o etapas: a) La cesión y transferencia de datos personales se realizará a solicitud de una persona legalmente autorizada; b) La solicitud deberá contener el objeto y la finalidad que se persigue con dicha información; c) El responsable del fichero de datos deberá cumplir con las medidas de seguridad y confidencialidad de los datos personales, verificando que el solicitante cumpla de igual manera con estas medidas; d) El responsable del fichero de datos personales deberá informar a la persona titular de los datos, la solicitud de transferencia y el propósito que se persigue, para su consentimiento; con las excepciones contenidas en el artículo anterior; e) El solicitante y el responsable del fichero de datos, deberán evitar que la información suministrada sea enviada a terceras personas; y f) El responsable del fichero de datos deberá informar a la Dirección de Protección de Datos Personales, la transferencia de datos realizada.

El Capítulo III titulado "Derechos del titular de los datos", aborda en el artículo 16, el Derecho a solicitar información a la Dirección de Protección de Datos Personales, relativa a la existencia de ficheros de datos personales, sus finalidades y la identidad de sus responsables. Agregando que el registro que se lleve al efecto será de consulta pública y gratuita.

La letra b) del artículo 17 además consagra el derecho del titular de los datos a rectificar, modificar, suprimir, complementar, incluir, actualizar o cancelar sus datos personales. Y el artículo 18 se refiere al Derechos de modificación de los datos.

El Capítulo IV se titula "Ficheros y responsables de ficheros de datos personales", regulando entre los artículos 22 al 27, la obligatoriedad de inscripción en el registro de ficheros de datos, los Ficheros de datos público y privado, la excepcionalidad en el uso de los datos personales, los ficheros de datos destinados al envío de publicidad, promociones, ofertas y venta directa de productos, bienes y servicios, el envío de publicidad y los datos relativos a las encuestas.

El Capítulo V titulado "De la Dirección de Protección de Datos Personales", se refiere a la autoridad de control en materia de protección de datos y las funciones de la misma, señalando el artículo 28 que la Dirección de Protección de Datos Personales adscrita al Ministerio de Hacienda y Crédito Público, contará con un Director designado por la máxima autoridad administrativa de dicho ministerio cuyo objeto es el control, supervisión y protección del tratamiento de los datos personales contenidos en ficheros de datos de naturaleza pública y privada.

El artículo 31 establece la existencia de los inspectores, al señalar que La Dirección de Protección de Datos Personales, deberá tener personal calificado que realice la función de inspectores. A continuación el artículo 32 regula los procedimientos de inspección para los ficheros de datos tanto públicos como privados, disponiendo que "son actividades de visita,

verificación y control, mediante las cuales los inspectores debidamente identificados, están facultados para revisar los ficheros de datos de acuerdo al programa de visitas, y que se encuentren operando en el almacenamiento de datos, sean estos públicos y privados dentro del territorio nacional con el objetivo de establecer el grado de cumplimiento de las normas regulatorias de esta actividad o de brindar a las autoridades de la Dirección de Protección de Datos Personales mayores elementos de juicio para la adopción de una resolución con afectación a terceros o no".

El artículo 34 se refiere a las responsabilidades y atribuciones del inspector y entre los artículos 36 y 43 la ley regula los distintos aspectos relacionados con el procedimiento de inspección, tales como: el contenido del acta de inspección, la comprobación de infracciones, el tiempo de duración de la inspección, la prueba, la iniciación de la inspección, la inspección por denuncia, el contenido de la denuncia y el contenido de la orden de inspección.

El Capítulo VI sobre las "Infracciones y sanciones", distingue entre sanciones leves (artículo 44), sanciones graves (artículo 45) y sanciones administrativas (artículo 46).

El Capítulo VII titulado "De las acciones de protección de datos personales", aborda la vía administrativa para la tutela de la protección de datos personales, estableciendo el artículo 48 que la Dirección de Protección de Datos Personales, es el órgano encargado de conocer y resolver la acción de protección de datos personales mediante denuncia presentada por el titular en relación con el tratamiento de datos personales que lesionen alguno de los derechos contemplados en esta Ley.

En el año 2018 se aprueba La Ley N° 983, Ley de Justicia Constitucional, mediante la cual se introduce la regulación del recurso de habeas data como garantía de tutela de datos personales asentado en cualquier tipo de soporte de índole pública o privada.

El Capítulo VIII se refiere a las disposiciones transitorias y el Capítulo IX aborda las "Disposiciones finales", relativas al complemento reglamentario que tendrá la ley y a su entrada en vigor.

Panamá

La protección de datos de carácter personal es regulada por la Ley N° 81 sobre Protección de Datos Personales del 26 de marzo del año 2019, publicada en la Gaceta Oficial Digital 28743-A, el viernes 29 de marzo de 2019, por lo que es una de las más recientes leyes en la materia a nivel latinoamericano, la que comenzará a regir dos años después de su publicación, es decir el 30 de marzo del año 2021. Se estructura sobre siete capítulos en los que se contiene un total de cuarenta y siete artículos.

El Capítulo I sobre "Disposiciones Generales", en su artículo 1° hace referencia al objeto de la ley, señalando que "esta tiene por objeto establecer los principios, derechos, obligaciones y procedimientos que regulan la protección de datos personales considerado su interrelación con la vida privada y demás derechos y libertades fundamentales de los ciudadanos, por parte de las personas naturales o jurídicas, de derecho público o privado, lucrativas, lucrativas o no…"

El artículo 2° se refiere a los principios en los que se sustenta el tratamiento de datos personales, distinguiendo los principios de lealtad, finalidad, proporcionalidad, veracidad y exactitud, seguridad de los datos, transparencia, confidencialidad, licitud y portabilidad,

Sobre la confidencialidad, la ley establece que las bases de datos que contengan datos personales y que reposen en custodia del Estado deberán ser resguardadas de manera segura, ya sea que se encuentren ubicadas dentro o fuera del territorio nacional, como complemento a las legislaciones especiales que crean y reglamentan las bases de datos personales. En cuanto a los datos de importancia crítica estatal, se establece que los mismos deben hospedarse en servidores ubicados dentro del territorio nacional. En cuanto al principio de proporcionalidad establece que los datos personales sólo deberán ser solicitados si son adecuados, pertinentes y limitados al mínimo necesario en relación con la finalidad para lo que son requeridos.

El artículo 4° conceptualiza una serie de términos en su numeral 9, establece explícitamente la noción de dato personal como "cualquier información concerniente a personas naturales, que las identifica o las hace identificables". Otros numerales del mismo artículo proporcionan otras definiciones, como el numeral 6, señalando a los datos confidenciales como "aquellos datos que por su naturaleza no deben ser de conocimiento público o de terceros no autorizados, incluyendo aquellos que estén protegidos por ley, por acuerdo de confidencialidad o no divulgación, a fin de salvaguardar información". El artículo 4, en su numeral 11 define "Dato sensible" como "aquel que se refiera a la esfera íntima de su titular, o cuya utilización indebida pueda dar origen a discriminación o conlleve un riesgo grave para este." Se indica que los datos sensibles son aquellos sobre el origen racial o étnico; creencias o convicciones religiosas, filosóficas y morales; afiliación sindical; opiniones políticas; datos relativos a la salud, a la vida, a la preferencia u orientación sexual, datos genéticos o datos biométricos, entre otros.

El artículo 7 especifica las responsabilidades de los sujetos obligados, como el establecimiento de los protocolos y procedimientos de gestión y transferencia segura. En su artículo 9 se menciona la obligación de guardar la confidencialidad de los datos, y el artículo 14 establece la obligación de cuidar los datos con debida diligencia y designa las responsabilidades por daños o perjuicios ocasionados que le sean exigibles.

El Capítulo II "Derechos de los Titulares de Datos Personales", en su artículo 15 hace referencia a los Derechos de Acceso, Rectificación, Cancelación, Oposición y Portabilidad (ARCOP), los cuales pueden ser ejercidos en cualquier momento siendo estos irrenunciables salvo excepciones contempladas en las leyes especiales, estableciendo los siguientes derechos: Derecho de Acceso: permite al titular obtener sus datos personales que se encuentren almacenados o sujetos a tratamiento en bases de datos de instituciones públicas o privadas, además de conocer el origen y la finalidad para los cuales han sido recabados; Derecho de Rectificación: permite al titular solicitar la corrección de sus datos personales que sean incorrectos, irrelevantes, incompletos, desfasados, inexactos, falsos o impertinentes; Derecho de Cancelación: permite al titular solicitar la eliminación de sus datos personales incorrectos, irrelevantes, incompletos, desfasados, inexactos, falsos o impertinentes; Derecho de Oposición: permite al titular, por motivos fundados y legítimos relacionados con una situación en particular, negarse a proporcionar sus datos personales o a que sean objeto de determinado tratamiento, así como a revocar su consentimiento; y Derecho de Portabilidad: permite al titular obtener copia de los datos personales de manera estructurada, en formato genérico y de uso común, que permita ser operado por distintos sistemas y/o transmitirlos a otro responsable, cuando: 1. El titular haya entregado sus datos directamente al responsable. 2. Sea un volumen relevante de datos, tratados de forma automatizada 3. El titular haya dado su consentimiento para el tratamiento o se requiera para la ejecución o el cumplimiento de un contrato.

Como se puede apreciar esta categorización de derechos del titular de los datos tiene una fuerte influencia de la regulación europea en la materia, reconociendo por ejemplo el derecho a la portabilidad, derecho que no es reconocido en otras legislaciones latinoamericanas anteriores al RGPD.

El Capítulo III "Utilización de Datos Personales", en el artículo 25, aborda cuestiones relativas a la transferencia o cesión de datos al establecer que solo podrán trasmitir información sobre los mismos cuando cuenten con el consentimiento previo, informado e inequívoco del titular, salvo lo establecido en leyes especiales. En este sentido, hay que tomar en consideración lo establecido en el artículo 28 sobre la prohibición por parte del responsable del tratamiento de datos personales y/o el custodio de la base de datos, de transferir o comunicar los datos que se relacionen con una persona identificada o identificable, luego de transcurridos siete años desde que se extinguió la obligación legal de conservarla, salvo que el titular de los datos personales expresamente solicite lo contrario. Se aborda de igual manera en el artículo 31 que los responsables y/o custodios de bases de datos que transfieran datos personales almacenados en bases de datos a terceros, deben llevar un registro de estas. Estas bases de datos deberán estar a disposición de la ANTAI, Autoridad de Transparencia y Acceso a la Información, en caso de que esta lo requiera, para cumplir con las facultades que le otorga la presente Ley. Los artículos 29 y 30 abordan cuestiones inherentes al tratamiento de datos personales por parte de una entidad pública al indicarse expresamente que solo podrá efectuarse respecto de las materias de su competencia, y en los casos de condenas por delitos, infracciones administrativas o faltas disciplinarias; no podrán comunicarlos una vez prescrita la acción penal o administrativa o cumplida o prescrita la sanción o la pena, salvo autorización expresa por el titular del dato.

El Capítulo IV "Consejo de Protección de Datos Personales", crea esta entidad colegida de carácter consultivo y cuyas funciones están previstas en el artículo 35 de la ley, las cuales son: asesorar a la ANTAI, que es la autoridad de control en protección de datos, recomendando acciones y reglamentos; recomendar políticas públicas relacionadas con la materia; evaluar casos y proponer recomendaciones; y desarrollar su reglamento interno.

El Capítulo V "Responsabilidad y Sanciones", el artículo 36 otorga facultades a la ANTAI "para sancionar a la persona natural o jurídica, responsable del tratamiento de los datos personales, así como también al custodio de la base de datos, que por razón de la investigación de las quejas o denuncias que se le presenten y se les compruebe que han infringido los derechos del titular de los datos personales". La ANTAI fijará los montos de las sanciones aplicables a las respectivas faltas, de conformidad a la gravedad de las faltas. También reglamentará el procedimiento correspondiente.

En el Capítulo VI "Infracciones y Sanciones", se consagran en el artículo 38 las infracciones, leves, graves y muy graves. En el artículo 42 se establece que "las sanciones que imponga la ANTAl a los responsables de las bases de datos y demás sujetos alcanzados por el régimen de la presente Ley y sus reglamentos, se graduarán en atención a la reincidencia de la infracción cometida. Las infracciones se clasifican así: leves, graves y muy graves. 1. Falta leve: citación ante la ANTAI respecto a registros o atender faltas. 2. Faltas graves: multas proporcionales a la falta. 3. Faltas muy graves: A. Clausura de los registros de las bases de datos, sin perjuicio de la multa correspondiente. B. Suspensión e inhabilitación de la actividad de almacenamiento y/o tratamiento de datos personales de forma temporal o permanente, sin perjuicio de la multa correspondiente. Para hacer cumplir la sanción de suspensión o clausura, la ANTAl podrá requerir el auxilio de la Fuerza Pública".

El Capítulo VIII "Disposiciones Finales", dispone en su artículo 45 que la ANTAI contará con los recursos presupuestarios y financieros para el debido cumplimiento de las funciones que se le atribuyen y el artículo 47 establece que la ley comenzará a regir dos años después de su promulgación.

Perú

El 21 de junio de 2011 se aprueba la Ley N° 29.733 Ley de Protección de Datos Personales LPDP, que dispone un conjunto de derechos y obligaciones que regulan la materia en Perú. Luego, el 21 de marzo de 2013 se aprueba mediante Decreto Supremo 003-2013-JUS, el respectivo reglamento de la señalada ley, los que fueron actualizados por el Decreto Legislativo N° 1353 del año 2017 que reformo aspectos relacionados con el régimen de la protección de datos en dicho país, creando la Autoridad de Transparencia y Acceso a la Información Pública, fortaleciendo el régimen de protección de datos personales y la regulación de la gestión de intereses. Señalando el inciso primero de su artículo 3 a propósito de la naturaleza jurídica y competencias de la Autoridad de control que: "El Ministerio de Justicia y Derechos Humanos a través de la Dirección Nacional de Transparencia y Acceso a Información Pública es la Autoridad Nacional de Transparencia y Acceso a la Información Pública, en adelante la Autoridad".

La LPDP se estructura en cuarenta artículos contenidos en un Título Preliminar, sobre "Disposiciones generales" y siete títulos. Título I: Principios rectores; Título II: Tratamiento de datos personales; Título III: Derechos del titular de datos personales; Título IV: Obligaciones del titular y del encargado del banco de datos personales; Título V: Bancos de datos personales; Título VI: Autoridad Nacional de Protección de Datos Personales; Título VII: Infracciones y sanciones administrativas, y once disposiciones complementarias finales.

El artículo 1° de la ley se refiere a su objeto, al señalar que esta persigue "garantizar el derecho fundamental a la protección de los datos personales, previsto en el artículo 2 numeral 6 de la Constitución Política del Perú, a través de su adecuado tratamiento, en un marco de respeto de los demás derechos fundamentales que en ella se reconocen".

El artículo 2 de la ley, se refiere a una serie de términos que define, entre los cuales es posible destacar en el número 4 a los Datos personales, como "Toda información sobre una persona natural que la identifica o la hace identificable a través de medios que pueden ser razonablemente utilizados". En el número 5 a los Datos sensibles, como "Datos personales constituidos por los datos biométricos que por sí mismos pueden identificar al titular; datos referidos al origen racial y étnico; ingresos económicos, opiniones o convicciones políticas, religiosas, filosóficas o morales; afiliación sindical; e información relacionada a la salud o a la vida sexual". En el número 6 al Encargado del banco de datos personales, que lo define como "Toda persona natural, persona jurídica de derecho privado o entidad pública que sola o actuando conjuntamente con otra realiza el tratamiento de los datos personales por encargo del titular del banco de datos personales".

El artículo 3 de la ley se refiere a su ámbito de aplicación, en efecto, la ley se aplica a los datos personales contenidos o destinados a ser contenidos en bancos de datos personales tanto de la administración pública y de administración privada, cuyo tratamiento se realiza en el territorio nacional. Son objeto de especial protección los datos sensibles. Señala que sus disposiciones no se aplican a los siguientes datos personales: 1. A los contenidos o destinados a ser contenidos en bancos de datos personales creados por personas naturales para fines

exclusivamente relacionados con su vida privada o familiar, y 2. A los contenidos o destinados a ser contenidos en bancos de datos de administración pública, solo en tanto su tratamiento resulte necesario para el estricto cumplimiento de las competencias asignadas por ley a las respectivas entidades públicas, para la defensa nacional, seguridad pública, y para el desarrollo de actividades en materia penal para la investigación y represión del delito.

El Título I sobre los principios rectores, distingue entre el Principio de legalidad, el Principio de consentimiento, el Principio de finalidad, el Principio de proporcionalidad, el Principio de calidad, el Principio de seguridad, el Principio de disposición de recurso y el Principio de nivel de protección adecuado. Además, en el artículo 12 se refiere al valor de los principios, al señalar que: "La actuación de los titulares y encargados de los bancos de datos personales y, en general, de todos los que intervengan con relación a datos personales, debe ajustarse a los principios rectores a que se refiere este Título. Esta relación de principios rectores es enunciativa. Los principios rectores señalados sirven también de criterio interpretativo para resolver las cuestiones que puedan suscitarse en la aplicación de esta Ley y de su reglamento, así como de parámetro para la elaboración de otras disposiciones y para suplir vacíos en la legislación sobre la materia".

El Titulo II sobre el "Tratamiento de datos personales", aborda en el artículo 13 el alcance de dicho tratamiento, en el artículo 14 regula las limitaciones al consentimiento para el tratamiento de datos personales, señalando que no se requiere el consentimiento del titular de datos personales, para los efectos de su tratamiento, en los siguientes casos: 1. Cuando los datos personales se recopilen o transfieran para el ejercicio de las funciones de las entidades públicas en el ámbito de sus competencias. 2. Cuando se trate de datos personales contenidos o destinados a ser contenidos en fuentes accesibles para el público. 3. Cuando se trate de datos personales relativos a la solvencia patrimonial y de crédito, conforme a ley. 4. Cuando medie norma para la promoción de la competencia en los mercados regulados emitida en ejercicio de la función normativa por los organismos reguladores a que se refiere la Ley 27332, Ley Marco de los Organismos Reguladores de la Inversión Privada en los Servicios Públicos, o la que haga sus veces, siempre que la información brindada no sea utilizada en perjuicio de la privacidad del usuario. 5. Cuando los datos personales sean necesarios para la ejecución de una relación contractual en la que el titular de datos personales sea parte, o cuando se trate de datos personales que deriven de una relación científica o profesional del titular y sean necesarios para su desarrollo o cumplimiento. 6. Cuando se trate de datos personales relativos a la salud y sea necesario, en circunstancia de riesgo, para la prevención, diagnóstico y tratamiento médico o quirúrgico del titular, siempre que dicho tratamiento sea realizado en establecimientos de salud o por profesionales en ciencias de la salud, observando el secreto profesional; o cuando medien razones de interés público previstas por ley o cuando deban tratarse por razones de salud pública, ambas razones deben ser calificadas como tales por el Ministerio de Salud; o para la realización de estudios epidemiológicos o análogos, en tanto se apliquen procedimientos de disociación adecuados. 7. Cuando el tratamiento sea efectuado por organismos sin fines de lucro cuya finalidad sea política, religiosa o sindical y se refiera a los datos personales recopilados de sus respectivos miembros, los que deben guardar relación con el propósito a que se circunscriben sus actividades, no pudiendo ser transferidos sin consentimiento de aquellos. 8. Cuando se hubiera aplicado un procedimiento de anonimización o disociación. 9. Cuando el tratamiento de los datos personales sea necesario para salvaguardar intereses legítimos del titular de datos personales por parte del titular de datos personales o por

el encargado de datos personales y 10. Otros establecidos por ley, o por el reglamento otorgado de conformidad con la presente Ley.

Por su parte el artículo 17 se refiere a la confidencialidad de los datos personales al señalar que el titular del banco de datos personales, el encargado y quienes intervengan en cualquier parte de su tratamiento están obligados a guardar confidencialidad respecto de estos y de sus antecedentes. Esta obligación subsiste aun después de finalizadas las relaciones con el titular del banco de datos personales. El obligado puede ser relevado de la obligación de confidencialidad cuando medie consentimiento previo, informado, expreso e inequívoco del titular de los datos personales, resolución judicial consentida o ejecutoriada, o cuando medien razones fundadas relativas a la defensa nacional, seguridad pública o sanidad pública, sin perjuicio del derecho a guardar el secreto profesional.

El Titulo III "Derechos del Titular de Datos Personales", se refiere a estos entre los artículos 18 al 25, distingüendo entre el Derecho de información del titular de datos personales, el Derecho de acceso del titular de datos personales, el Derecho de actualización, inclusión, rectificación y supresión, el Derecho a impedir el suministro, el Derecho de oposición, el Derecho al tratamiento objetivo, el Derecho a la tutela, y el Derecho a ser indemnizado.

El artículo 27 aborda las limitaciones para el ejercicio de éstos derechos al señalar que:

> *"Los titulares y encargados de los bancos de datos personales de administración pública pueden denegar el ejercicio de los derechos de acceso, supresión y oposición por razones fundadas en la protección de derechos e intereses de terceros o cuando ello pueda obstaculizar actuaciones judiciales o administrativas en curso vinculadas a la investigación sobre el cumplimiento de obligaciones tributarias o previsionales, a las investigaciones penales sobre la comisión de faltas o delitos, al desarrollo de funciones de control de la salud y del medio ambiente, a la verificación de infracciones administrativas, o cuando así lo disponga la ley".*

El Título IV sobre "Obligaciones del Titular y del Encargado del Banco de Datos Personales", sobre este punto hay que precisar que el numeral sexto del artículo 2 de la propia ley define al Encargado del banco de datos personales como "Toda persona natural, persona jurídica de derecho privado o entidad pública que sola o actuando conjuntamente con otra realiza el tratamiento de los datos personales por encargo del titular del banco de datos personales".

Sobre las obligaciones tanto del titular como el encargado del banco de datos se refiere el artículo 28 de la ley.

> *"Artículo 28. Obligaciones El titular y el encargado del banco de datos personales, según sea el caso, tienen las siguientes obligaciones: 1. Efectuar el tratamiento de datos personales, solo previo consentimiento informado, expreso e inequívoco del titular de los datos personales, salvo ley autoritativa, con excepción de los supuestos consignados en el artículo 14 de la presente Ley. 2. No recopilar datos personales por medios fraudulentos, desleales o ilícitos. 3. Recopilar datos personales que sean actualizados, necesarios, pertinentes y adecuados, con relación a finalidades determinadas, explícitas y lícitas para las que se hayan obtenido. 4. No utilizar los datos personales objeto de tratamiento para finalidades distintas de aquellas que motivaron su recopilación, salvo que medie procedimiento de anonimización o disociación. 5. Almacenar los datos personales de manera que se posibilite el ejercicio de los derechos de su titular. 6. Suprimir y sustituir o, en su caso, completar los datos*

> *personales objeto de tratamiento cuando tenga conocimiento de su carácter inexacto o incompleto, sin perjuicio de los derechos del titular al respecto. 7. Suprimir los datos personales objeto de tratamiento cuando hayan dejado de ser necesarios o pertinentes a la finalidad para la cual hubiesen sido recopilados o hubiese vencido el plazo para su tratamiento, salvo que medie procedimiento de anonimización o disociación. 8. Proporcionar a la Autoridad Nacional de Protección de Datos Personales la información relativa al tratamiento de datos personales que esta le requiera y permitirle el acceso a los bancos de datos personales que administra, para el ejercicio de sus funciones, en el marco de un procedimiento administrativo en curso solicitado por la parte afectada. 9. Otras establecidas en esta Ley y en su reglamento"*.

El Título V, sobre "Bancos de Datos Personales", se refiere a la creación, modificación o cancelación de bancos de datos personales, respecto de los cuales sean de datos personales de administración pública y de administración privada, se sujetan a lo que establezca el reglamento, salvo la existencia de disposiciones especiales contenidas en otras leyes. En todo caso, se garantiza la publicidad sobre su existencia, finalidad, identidad y el domicilio de su titular y, de ser el caso, de su encargado.

El Título VI aborda la Autoridad Nacional de Protección de Datos Personales, disponiendo en el Artículo 32 que la autoridad de control es el Ministerio de Justicia, a través de la Dirección Nacional de Justicia, y que por lo tanto esta se constituye como la Autoridad Nacional de Protección de Datos Personales, la que, para el adecuado desempeño de sus funciones, puede crear oficinas en todo el país. La Autoridad Nacional de Protección de Datos Personales se rige por lo dispuesto en esta Ley, en su reglamento y en los artículos pertinentes del Reglamento de Organización y Funciones del Ministerio de Justicia.

Corresponde a la Autoridad Nacional de Protección de Datos Personales realizar todas las acciones necesarias para el cumplimiento del objeto y demás disposiciones de la LPDP y de su reglamento. Para tal efecto, goza de potestad sancionadora, de conformidad con la Ley 27.444, que es la ley del Procedimiento Administrativo General, o la que haga sus veces, así como de potestad coactiva, de conformidad con la ley 26.979, que es la Ley de Procedimiento de Ejecución Coactiva, o la que haga sus veces.

La Autoridad Nacional de Protección de Datos Personales debe presentar periódicamente un informe sobre sus actividades al Ministro de Justicia. Para el cumplimiento de sus funciones, la Autoridad Nacional de Protección de Datos Personales cuenta con el apoyo y asesoramiento técnico de la Oficina Nacional de Gobierno Electrónico e Informática (ONGEI) de la Presidencia del Consejo de Ministros, o la que haga sus veces.

El artículo 33 se refiere a las funciones que tendrá la Autoridad Nacional de Protección de Datos Personales y el artículo 36 a los recursos con los que contará, distinguiendo: 1. Las tasas por concepto de derecho de trámite de los procedimientos administrativos y servicios de su competencia. 2. Los montos que recaude por concepto de multas. 3. Los recursos provenientes de la cooperación técnica internacional no reembolsable. 4. Los legados y donaciones que reciba. 5. Los recursos que se le transfieran conforme a ley.

Luego, en el inciso final del artículo 36, dispone que "Los recursos de la Autoridad Nacional de Protección de Datos Personales son destinados a financiar los gastos necesarios para el desarrollo de sus operaciones y para su funcionamiento.

El Título VII "Infracciones y Sanciones Administrativas", regula el procedimiento sancionador, en efecto, se desprende del artículo 37 de la ley que; "El procedimiento sancionador se inicia de oficio, por la Autoridad Nacional de Protección de Datos Personales o por denuncia de parte, ante la presunta comisión de actos contrarios a lo dispuesto en la presente Ley o en su reglamento, sin perjuicio del procedimiento seguido en el marco de lo dispuesto en el artículo 24.

> *"Artículo 24. Derecho a la tutela En caso de que el titular o el encargado del banco de datos personales deniegue al titular de datos personales, total o parcialmente, el ejercicio de los derechos establecidos en esta Ley, este puede recurrir ante la Autoridad Nacional de Protección de Datos Personales en vía de reclamación o al Poder Judicial para los efectos de la correspondiente acción de hábeas data. El procedimiento a seguir ante la Autoridad Nacional de Protección de Datos Personales se sujeta a lo dispuesto en los artículos 219 y siguientes de la Ley 27.444, Ley del Procedimiento Administrativo General, o la que haga sus veces. La resolución de la Autoridad Nacional de Protección de Datos Personales agota la vía administrativa y habilita la imposición de las sanciones administrativas previstas en el artículo 39. El reglamento determina las instancias correspondientes. Contra las resoluciones de la Autoridad Nacional de Protección de Datos Personales procede la acción contencioso-administrativa".*

Las resoluciones de la Autoridad Nacional de Protección de Datos Personales agotan la vía administrativa. Contra las resoluciones de la Autoridad Nacional de Protección de Datos Personales procede la acción contencioso-administrativa".

El artículo 38 se refiere a los distintos tipos de infracciones, leves, graves y muy graves. Así como las sanciones administrativas (artículo 39) y las multas correctivas (artículo 40).

República Dominicana

En este país la protección de datos está regulada en la Ley N° 172-13 que tiene por objeto la protección integral de los datos personales asentados en archivos, registros públicos, bancos de datos u otros medios técnicos de tratamiento de datos destinados a dar informes, sean estos públicos o privados, publicada el 15 de diciembre de 2013.

La señalada ley se estructura en seis capítulos en los que se contienen 91 artículos. El Capítulo I "Disposiciones Iníciales", en su Sección I se refiere al objeto, alcance, ámbito de aplicación, restricciones y principios. El artículo 1° establece el objeto de la ley cual es;

> *"la protección integral de los datos personales asentados en archivos, registros públicos, bancos de datos u otros medios técnicos de tratamiento de datos destinados a dar informes, sean éstos públicos o privados, así como garantizar que no se lesione el derecho al honor y a la intimidad de las personas, y también facilitar el acceso a la información que sobre las mismas se registre, de conformidad a lo establecido en el Artículo 44*[449] *de la Constitución de la República Dominicana.*

[449] "Toda persona tiene derecho a la intimidad. Se garantiza el respeto y la no injerencia en la vida privada, familiar, el domicilio y la correspondencia del individuo. Se reconoce el derecho al honor, al buen nombre y a la propia imagen. Toda autoridad o particular que los viole está obligado a resarcirlos o repararlos conforme a la ley. Por tanto: 2) Toda persona tiene el derecho a acceder a la información y a los datos que sobre ella o sus bienes

> *Del mismo modo, regula la constitución, organización, actividades, funcionamiento y extinción de las Sociedades de Información Crediticia (SIC), así como la prestación de los servicios de referencias crediticias y el suministro de la información en el mercado, garantizando el respeto a la privacidad y los derechos de los titulares de esta, promoviendo la veracidad, la precisión, la actualización efectiva, la confidencialidad y el uso apropiado de dicha información.*
> *En ningún caso se afectarán las fuentes de información periodísticas".*

El artículo 5° aborda los principios en los que se sustenta la protección de datos, distinguiendo entre: Licitud de los archivos de datos personales, Calidad de los datos, Derecho de información, Consentimiento del afectado, Seguridad de los datos, Deber de secreto, Lealtad y Finalidad de los datos.

La Sección II del Capítulo I se titula "Definiciones", donde se conceptualizan diversos términos, entre otros: "Consentimiento del interesado: Toda manifestación de voluntad, libre, inequívoca, específica e informada, mediante la que el interesado consiente el tratamiento de datos personales que le conciernen"; "Datos especialmente protegidos: Datos de carácter personal que revelan origen racial y étnico, opiniones políticas, convicciones religiosas, filosóficas o morales, afiliación sindical e información referente a la salud o a la vida sexual"; "Datos de carácter personal: Cualquier información numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo concerniente a personas físicas identificadas o identificables"; "Datos de carácter personal relacionados con la salud: Cualquier información concerniente a la salud pasada, presente y futura, física o mental, de un individuo"; "Destinatario o cesionario: Persona física o jurídica, pública o privada, u órgano administrativo, al que se revelen los datos"; "Encargado del tratamiento: La persona física o jurídica, pública o privada, que realice el tratamiento de los datos personales por cuenta del responsable del tratamiento"; "Datos del historial de crédito o datos crediticios: Información relativa al historial crediticio de una persona física o jurídica, así como cualquier otra información suministrada por la Superintendencia de Bancos u otras de carácter y dominio público, ya sea por su procedencia o por su naturaleza"; "Datos informáticos: Los datos personales sometidos al tratamiento o procesamiento electrónico o automatizado"; y "Datos sensibles: Datos personales que revelan las opiniones políticas, las convicciones religiosas, filosóficas o morales, la afiliación sindical e información referente a la salud o a la vida sexual".

El Capítulo II "Disposiciones Generales", en su Sección I regula los Derechos de las personas y su ejercicio. En efecto, entre los artículos 7 al 28, la ley consagra un conjunto de derechos del titular de los datos, así como un procedimiento para su tutela y ejercicio. Distingüendo entre el Derecho de consulta para la protección de datos; el Derecho de acceso; los Derechos de rectificación y cancelación y el Derecho a indemnización.

El artículo 17 se refiere a la Acción de hábeas data, que procederá para tomar conocimiento de la existencia de los datos personales almacenados en archivos, registros o bancos de datos públicos o privados que se deriven de una relación comercial, laboral o contractual con una

reposen en los registros oficiales o privados, así como conocer el destino y el uso que se haga de los mismos, con las limitaciones fijadas por la ley. El tratamiento de los datos e informaciones personales o sus bienes deberá hacerse respetando los principios de calidad, licitud, lealtad, seguridad y finalidad. Podrá solicitar ante la autoridad judicial competente la actualización, oposición al tratamiento, rectificación o destrucción de aquellas informaciones que afecten ilegítimamente sus derechos".

entidad pública o privada, o simplemente, para tomar conocimiento de los datos personales que se presuma que existen almacenados en archivos, registros o bancos de datos públicos o privados. En los casos en que se presuma inexactitud, la desactualización de la información de que se trata, o el tratamiento de datos cuyo registro se encuentre prohibido en la presente ley, para exigir su rectificación, supresión o actualización.

Entre los artículos 21 al 25 se dispone el procedimiento aplicable para el ejercicio de la acción de habeas data, distinguiéndose entre el trámite de la demanda, la contestación del informe, ampliación de la demanda y el Procedimiento de reclamación aplicable a las Sociedades de Información Crediticia (SIC) para la modificación, rectificación y cancelación de la información del titular.

El Capítulo III "Disposiciones Orgánicas", En su Sección I se refiere al Órgano de Control. Estableciendo su artículo 29 que: "Los archivos, registros o bancos de datos, públicos o privados, destinados a proveer informes crediticios estarán sujetos a la inspección y vigilancia de la Superintendencia de Bancos como órgano de control. El órgano de control deberá realizar todas las acciones necesarias para el cumplimiento de los objetivos y demás disposiciones de la presente ley. A tales efectos, tendrá las siguientes funciones y atribuciones: 1. Asistir y asesorar a las personas físicas que lo requieran acerca de los alcances y de los medios legales de que disponen para la defensa de los derechos que ésta garantiza. 2. Imponer las sanciones administrativas que en su caso correspondan por violación a las normas establecidas".

De lo expuesto, es posible apreciar que la presente ley tiene un enfoque principal en el tratamiento de datos personales realizado por las entidades crediticias y carece de una autoridad administrativa con facultades normativas que supervise la aplicación de esta, y en particular, ejerza las funciones de vigilancia para el cumplimiento efectivo de las políticas sobre protección de datos que establezca.

El Capítulo IV "Disposiciones Procedimentales" en su Sección I se refiere a los Ficheros de Titularidad Pública, estableciendo el artículo 37 que la "La creación, modificación o supresión de los archivos de datos personales de la administración pública sólo puede hacerse por medio de las disposiciones contenidas en la Ley de Función Pública, y por medio de la Ley General de Libre Acceso a la Información Pública". En la Sección II se abordan los ficheros de las fuerzas armadas, de seguridad y organismos policiales o de inteligencia, en la Sección III los ficheros de titularidad privada y en la Sección IV sobre Otros Datos, se distingue la Subsección I sobre datos especialmente protegidos, la Subsección II sobre datos relativos a la salud y la Subsección III sobre el tratamiento de datos de menores de edad. En la Sección V del Capítulo IV se regula el Movimiento Internacional de Datos.

El Capítulo V "Disposiciones de Infracciones y Sanciones", en su artículo 81 distingue entre sanciones administrativas, el artículo 84 se refiere a las sanciones excepcionales, el artículo 85 a las sanciones civiles y el artículo 86 a las sanciones penales.

> *"Artículo 81. Sanciones administrativas. El órgano competente para sancionar las infracciones administrativas cometidas por las Sociedades de Información Crediticia (SIC) será la Superintendencia de Bancos: 1. Se consideran infracciones administrativas a la presente ley: a) Incluir en los reportes de crédito cualquiera de las informaciones prohibidas a las Sociedades de Información Crediticia (SIC), enumeradas en la presente ley. b) Negarse a facilitar el acceso a la información crediticia al titular de la misma. c) Denegar, sin fundamento, una solicitud de revisión*

o una solicitud de rectificación de la información crediticia requerida por el titular de la información. d) Negarse a modificar o a cancelar la información de un titular de la información, luego de que éste haya obtenido un pronunciamiento favorable en un procedimiento seguido de conformidad con lo establecido en la presente ley. 2. La Superintendencia de Bancos impondrá a las Sociedades de Información Crediticia (SIC) las sanciones administrativas siguientes: a) Cuando la Sociedad de Información Crediticia (SIC) infrinja de manera grave o reiterada las disposiciones de las sentencias de los tribunales con la autoridad de la cosa irrevocablemente juzgada, al tenor del Código Civil de la República Dominicana, violaciones que se deriven de las infracciones tipificadas en el acápite anterior, la Superintendencia de Bancos impondrá una multa de diez (10) a cien (100) salarios mínimos, que deberá ser pagada a partir de tres (3) días hábiles después de haber recibido dicha notificación. b) Cuando las Sociedades de Información Crediticia (SIC) no inicien las actividades dentro de los seis (6) meses posteriores a la fecha en que la autorización les haya sido otorgada por la Junta Monetaria, la Superintendencia de Bancos retirará o revocará el permiso de operación".

"Artículo 84. Sanciones excepcionales. Será sancionado con una multa de diez (10) a cincuenta (50) salarios mínimos vigentes, sin perjuicio de las reparaciones que procedan por los daños y perjuicios que haya sufrido la persona por causa de violación a su derecho a la privacidad, conforme a las normas del derecho común, la persona física que: 1. Insertará o hiciera insertar, a sabiendas, datos falsos en un archivo de datos personales, de manera dolosa o de mala fe. 2. Proporcionará, de manera dolosa o de mala fe, información falsa a un tercero, contenida en un archivo de datos personales. 3. Accediere a sabiendas e ilegítimamente, o violando sistemas de confidencialidad y seguridad de datos, de cualquier forma, a un banco de datos personales. 4. Revelare a otra información registrada en un banco de datos personales cuyo secreto estuviere obligado a preservar por disposición de una ley".

"Artículo 85. Sanciones civiles. Agotado el procedimiento de solicitud y rectificación establecido en la presente ley, se considerarán infracciones civiles: 1. Denegar, sin fundamento, una solicitud de revisión o una solicitud de rectificación de la información crediticia requerida por el titular de la información. 2. Negarse a modificar o a cancelar la información de un titular de la información, luego de que éste haya obtenido un pronunciamiento favorable en un procedimiento seguido de conformidad con lo establecido en la presente ley. 3. Infringir de manera grave o reiterada las disposiciones de las sentencias de los tribunales civiles con la autoridad de la cosa irrevocablemente juzgada".

"Artículo 86. Sanciones penales. En caso de que un usuario o suscriptor haya accedido a una base de datos para consultar, de manera fraudulenta, las informaciones personales de un titular sin haber obtenido de éste autorización previa, será sancionado con multa que irá de diez (10) a cincuenta (50) salarios mínimos vigentes, sin perjuicio de las reparaciones que procedan por los daños y perjuicios que haya sufrido la persona por causa de violación a su derecho a la privacidad, conforme a las normas del derecho común. Al usuario o suscriptor o cualquier persona física que

> *utilice o facilite un reporte de crédito proveniente de una Sociedad de Información Crediticia (SIC), con la finalidad de la comisión de un delito, se impondrá una sanción equivalente a prisión correccional de seis meses a dos años, y en caso de que haya tenido como finalidad facilitar la comisión de un crimen, será sancionado con la prisión que establezca el Código Penal vigente para los cómplices. Se considerará una circunstancia agravante del crimen imputado el hecho de que un usuario o suscriptor haga uso de un reporte de crédito proveniente de una Sociedad de Información Crediticia (SIC), con la finalidad de la comisión de un crimen. El usuario o suscriptor que dé al reporte de crédito un uso distinto al que se haya consignado en la autorización del cliente o consumidor, será sancionado con multa que irá de diez (10) a cien (100) salarios mínimos vigentes, sin perjuicio de las reparaciones que procedan por los daños y perjuicios que haya sufrido la persona por causa de violación a su derecho a la privacidad, conforme a las normas del derecho común".*

El Capítulo VI sobre "Disposiciones Transitorias y Finales", aborda en la Sección I "Disposiciones Transitorias" el Tratamientos de datos por convenios internacionales, estableciendo que todo lo relacionado con la protección de las personas físicas, en lo que respecta al tratamiento de datos de carácter personal, en relación con cualquier convenio o tratado internacional del que sea signataria la República Dominicana, se regirá conforme a las disposiciones de esta ley.

Por último, la Sección II establece la derogación de toda otra norma relacionada con las materias tratadas en sus disposiciones.

Uruguay

El 18 de agosto del año 2018, se publica en el Diario Oficial de la República Oriental del Uruguay, la Ley N° 18.331 sobre "Protección de Datos Personales y Habeas Data". Esta ley consta de 49 artículos contenidos en IX capítulos, el Capítulo I se titula "Disposiciones Generales", en su artículo 1° dispone que "El derecho a la protección de datos personales es inherente a la persona humana", por lo que está comprendido en el Constitución. En su artículo 2, establece que "El derecho a la protección de los datos personales se aplicará por extensión a las personas jurídicas, en cuanto corresponda". Y a continuación en el artículo 3, se dispone en relación con el ámbito de aplicación de esta, que, "El régimen de la presente ley será de aplicación a los datos personales registrados en cualquier soporte que los haga susceptibles de tratamiento, y a toda modalidad de uso posterior de estos datos por los ámbitos público o privado. No se aplicará a las siguientes bases de datos: a) A las mantenidas por personas físicas en el ejercicio de actividades exclusivamente personales o domesticas; b) Las que tengan por objeto la seguridad pública, la defensa, la seguridad del Estado y sus actividades en materia penal, investigación y represión del delito, y c) A las bases de datos creadas y reguladas por leyes especiales.

El artículo 4 al igual que otras legislaciones latinoamericanas, aborda una serie de términos de los cuales entrega una definición.

El Capítulo II se refiere a los Principios Generales, señalando su artículo 5 que "La actuación de los responsables de las bases de datos, tanto públicos como privados, y, en general, de todos quienes actúen en relación a datos personales de terceros, deberá ajustarse a los siguientes principios generales: a) Legalidad; b) Veracidad; c) Finalidad; d) Previo consentimiento

informado; e) Seguridad de los datos; f) Reserva y g) Responsabilidad. Dichos principios generales servirán también de criterio interpretativo para resolver las cuestiones que puedan suscitarse en la aplicación de las disposiciones pertinentes".

El Capítulo III aborda los Derechos de los Titulares de los Datos, distinguiendo entre: el Derecho de información frente a la recolección de datos (artículo 13); el Derecho de acceso (artículo 14); el Derecho de rectificación, actualización, inclusión o supresión (artículo 15); el Derecho a la impugnación de valoraciones personales (artículo 16) y los Derechos referentes a la comunicación de datos (artículo 17), que se relación con el principio de finalidad y el del consentimiento del titular de los datos. En efecto, Los datos personales objeto de tratamiento solo podrán ser comunicados para el cumplimiento de los fines directamente relacionados con el interés legítimo del emisor y del destinatario y con el previo consentimiento del titular de los datos, al que se le debe informar sobre la finalidad de la comunicación e identificar al destinatario o los elementos que permitan hacerlo. El previo consentimiento para la comunicación es revocable.

El previo consentimiento no será necesario cuando: así lo disponga una ley de interés general; en los supuestos del artículo 9; Se trate de datos personales relativos a la salud y sea necesario por razones de salud e higiene públicas, de emergencia o para la realización de estudios epidemiológicos, en tanto se preserve la identidad de los titulares de los datos mediante mecanismos de disociación adecuados, y se hubiera aplicado un procedimiento de disociación de la información, de modo que los titulares de los datos no sean identificables.

> *"Artículo 9º: Principio del previo consentimiento informado. - El tratamiento de datos personales es lícito cuando el titular hubiere prestado su consentimiento libre, previo, expreso e informado, el que deberá documentarse.*
> *El referido consentimiento prestado con otras declaraciones deberá figurar en forma expresa y destacada, previa notificación al requerido de datos, de la información descrita en el artículo 12 de la presente ley.*
> *No será necesario el previo consentimiento cuando: A) Los datos provengan de fuentes públicas de información, tales como registros o publicaciones en medios de comunicación masiva; B) Se recaben para el ejercicio de funciones propias de los poderes del Estado o en virtud de una obligación legal; C) Se trate de listados cuyos datos se limiten en el caso de personas físicas a nombres y apellidos, documento de identidad, nacionalidad, domicilio y fecha de nacimiento. En el caso de personas jurídicas, razón social, nombre de fantasía, registro único de contribuyentes, domicilio, teléfono e identidad de las personas a cargo de la misma; D) Deriven de una relación contractual, científica o profesional del titular de los datos, y sean necesarios para su desarrollo o cumplimiento; E) Se realice por personas físicas o jurídicas, privadas o públicas, para su uso exclusivo personal o doméstico"*.

El destinatario quedará sujeto a las mismas obligaciones legales y reglamentarias del emisor y este responderá solidaria y conjuntamente por la observancia de las mismas ante el organismo de control y el titular de los datos de que se trate.

El Capítulo IV aborda los "Datos Especialmente Protegidos", regulando el artículo 18 el tratamiento de los datos sensibles, al señalar que ninguna persona puede ser obligada a proporcionar datos sensibles. Éstos sólo podrán ser objeto de tratamiento con el consentimiento expreso y escrito del titular. Los datos sensibles sólo pueden ser recolectados y objeto de tratamiento cuando medien razones de interés general autorizadas por ley, o cuando el

organismo solicitante tenga mandato legal para hacerlo. También podrán ser tratados con finalidades estadísticas o científicas cuando se disocien de sus titulares.

Queda prohibida la formación de bases de datos que almacenen información que directa o indirectamente revele datos sensibles. Se exceptúan aquellos que posean los partidos políticos, sindicatos, iglesias, confesiones religiosas, asociaciones, fundaciones y otras entidades sin fines de lucro, cuya finalidad sea política, religiosa, filosófica, sindical, que hagan referencia al origen racial o étnico, a la salud y a la vida sexual, en cuanto a los datos relativos a sus asociados o miembros, sin perjuicio que la comunicación de dichos datos precisará siempre el previo consentimiento del titular del dato.

Los datos personales relativos a la comisión de infracciones penales, civiles o administrativas sólo pueden ser objeto de tratamiento por parte de las autoridades públicas competentes, en el marco de las leyes y reglamentaciones respectivas, sin perjuicio de las autorizaciones que la ley otorga u otorgare. Nada de lo establecido en esta ley impedirá a las autoridades públicas comunicar o hacer pública la identidad de las personas físicas o jurídicas que estén siendo investigadas por, o hayan cometido, infracciones a la normativa vigente, en los casos en que otras normas lo impongan o en los que lo consideren conveniente.

A continuación, en los artículos 19 y 20 se regula el tratamiento de datos relativos a la salud y a las telecomunicaciones respectivamente. En relación con el tratamiento de Datos relativos a la salud, se dispone que los establecimientos sanitarios públicos o privados y los profesionales vinculados a las ciencias de la salud pueden recolectar y tratar los datos personales relativos a la salud física o mental de los pacientes que acudan a los mismos o que estén o hubieren estado bajo tratamiento de aquéllos, respetando los principios del secreto profesional, la normativa específica y lo establecido en esta ley.

Sobre los Datos relativos a las telecomunicaciones, se dispone que los operadores que exploten redes públicas o que presten servicios de comunicaciones electrónicas disponibles al público deberán garantizar, en el ejercicio de su actividad, la protección de los datos personales conforme a esta ley. Igualmente, deberán adoptar las medidas técnicas y de gestiones adecuadas para preservar la seguridad en la explotación de su red o en la prestación de sus servicios, con el fin de garantizar sus niveles de protección de los datos personales que sean exigidos por la normativa de desarrollo de esta ley en esta materia. En caso de que exista un riesgo particular de violación de la seguridad de la red pública de comunicaciones electrónicas, el operador que explote dicha red o preste el servicio de comunicaciones electrónicas informará a los abonados sobre dicho riesgo y sobre las medidas a adoptar.

El artículo 22 se refiere a los Datos relativos a la actividad comercial o crediticia, señalando que:

> *"Queda expresamente autorizado el tratamiento de datos personales destinados a brindar informes objetivos de carácter comercial, incluyendo aquellos relativos al cumplimiento o incumplimiento de obligaciones de carácter comercial o crediticia que permitan evaluar la concertación de negocios en general, la conducta comercial o la capacidad de pago del titular de los datos, en aquellos casos en que los mismos sean obtenidos de fuentes de acceso público o procedentes de informaciones facilitadas por el acreedor o en las circunstancias previstas en la presente ley. Para el caso de las*

> *personas jurídicas, además de las circunstancias previstas en la presente ley, se permite el tratamiento de toda información autorizada por la normativa vigente.*
> *Los datos personales relativos a obligaciones de carácter comercial de personas físicas sólo podrán estar registrados por un plazo de cinco años contados desde su incorporación. En caso de que al vencimiento de dicho plazo la obligación permanezca incumplida, el acreedor podrá solicitar al responsable de la base de datos, por única vez, su nuevo registro por otros cinco años. Este nuevo registro deberá ser solicitado en el plazo de treinta días anteriores al vencimiento original. Las obligaciones canceladas o extinguidas por cualquier medio permanecerán registradas, con expresa mención de este hecho, por un plazo máximo de cinco años, no renovable, a contar de la fecha de la cancelación o extinción.*
> *Los responsables de las bases de datos se limitarán a realizar el tratamiento objetivo de la información registrada tal cual ésta le fuera suministrada, debiendo abstenerse de efectuar valoraciones subjetivas sobre la misma"*.

El Capítulo V se refiere a las "Bases de Datos de Titularidad Pública", regulando las bases de datos de las Fuerzas Armadas, Organismos Policiales o de Inteligencia, estableciendo el artículo 25 que: "los datos personales que por haberse almacenado para fines administrativos, deban ser objeto de registro permanente en las bases de datos de las fuerzas armadas, organismos policiales o de inteligencia; y aquellos sobre antecedentes personales que proporcionen dichas bases de datos a las autoridades administrativas o judiciales que los requieran en virtud de disposiciones legales", serán regulados por la señalada ley.

Además, dispone que el tratamiento de datos personales con fines de defensa nacional o seguridad pública por parte de las fuerzas armadas, organismos policiales o inteligencia, sin previo consentimiento de los titulares, queda limitado a aquellos supuestos y categoría de datos que resulten necesarios para el estricto cumplimiento de las misiones legalmente asignadas a aquéllos para la defensa nacional, la seguridad pública o para la represión de los delitos. Las bases de datos, en tales casos, deberán ser específicas y establecidas al efecto, debiendo clasificarse por categorías, en función de su grado de fiabilidad. Agregando que "Los datos personales registrados con fines policiales se cancelarán cuando no sean necesarios para las averiguaciones que motivaron su almacenamiento".

El artículo 26 se refiere a las excepciones al señalar que:

> *"Los responsables de las bases de datos que contengan los datos a que se refieren los incisos segundo y tercero del artículo anterior podrán denegar el acceso, la rectificación o cancelación en función de los peligros que pudieran derivarse para la defensa del Estado o la seguridad pública, la protección de los derechos y libertades de terceros o las necesidades de las investigaciones que se estén realizando.*
> *Los responsables de las bases de datos de la Hacienda Pública podrán, igualmente, denegar el ejercicio de los derechos a que se refiere el inciso anterior cuando el mismo obstaculice las actuaciones administrativas tendientes a asegurar el cumplimiento de las obligaciones tributarias y, en todo caso, cuando el titular del dato esté siendo objeto de actuaciones inspectivas.*

> *El titular del dato al que se deniegue total o parcialmente el ejercicio de los derechos mencionados en los incisos anteriores podrá ponerlo en conocimiento del Órgano de Control, quien deberá asegurarse de la procedencia o improcedencia de la denegación".*

El Capítulo VI se refiere a las "Bases de Datos de Titularidad Privada", derivándose del artículo 29 que:

> *"Toda base de datos pública o privada debe inscribirse en el Registro que al efecto habilite el Órgano de Control, de acuerdo con los criterios reglamentarios que se establezcan. Por vía reglamentaria se procederá a la regulación detallada de los distintos extremos que deberá contener la inscripción, entre los cuales figurarán necesariamente los siguientes: A) Identificación de la base de datos y el responsable de la misma; B) Naturaleza de los datos personales que contiene; C) Procedimientos de obtención y tratamiento de los datos; D) Medidas de seguridad y descripción técnica de la base de datos, E) Protección de datos personales y ejercicio de derechos; F) Destino de los datos y personas físicas o jurídicas a las que pueden ser transmitidos; G) Tiempo de conservación de los datos; H) Forma y condiciones en que las personas pueden acceder a los datos referidos a ellas y los procedimientos a realizar para la rectificación o actualización de los datos; I) Cantidad de acreedores personas físicas que hayan cumplido los 5 años previstos en el artículo 22 de la presente ley, y J) Cantidad de cancelaciones por incumplimiento de la obligación de pago si correspondiera, de acuerdo a lo previsto en el artículo 22 de la presente ley."*

El Capítulo VII aborda el "Órgano de Control", estableciendo el artículo 31 "Créase como órgano desconcentrado de la Agencia para el Desarrollo del Gobierno de Gestión Electrónica y la Sociedad de la Información y del Conocimiento (AGESIC), dotado de la más amplia autonomía técnica, la Unidad Reguladora y de Control de Datos Personales. Estará dirigida por un Consejo integrado por tres miembros: el Director Ejecutivo de AGESIC y dos miembros designados por el Poder Ejecutivo entre personas que, por sus antecedentes personales, profesionales y de conocimiento en la materia aseguren independencia de criterio, eficiencia, objetividad e imparcialidad en el desempeño de sus cargos.

A excepción del Director Ejecutivo de la AGESIC, los miembros durarán cuatro años en sus cargos, pudiendo ser designados nuevamente. Sólo cesarán por la expiración de su mandato y designación de sus sucesores, o por su remoción dispuesta por el Poder Ejecutivo en los casos de ineptitud, omisión o delito, conforme a las garantías del debido proceso. Durante su mandato no recibirán órdenes ni instrucciones en el plano técnico.

También en este capítulo se abordan las funciones, recursos y potestades sancionadoras que tendrá el órgano de control.

El Capítulo VIII regula la "Acción de Protección de Datos Personales", estableciendo su procedencia y competencia (artículo 38), la legitimación (artículo 39), el procedimiento (artículo 40) y el recurso de apelación y segunda instancia (artículo 44), entre otros.

El artículo 37 dispone:

> *"Habeas data, Toda persona tendrá derecho a entablar una acción judicial efectiva para tomar conocimiento de los datos referidos a su persona y de su finalidad y uso, que consten en bases de datos públicos o privados; y en caso de error, falsedad, prohibición de tratamiento, discriminación o desactualización a exigir su rectificación, inclusión, supresión o lo que entienda corresponder. Cuando se trate de datos personales cuyo registro esté amparado por una norma legal que consagre el secreto a su respecto, el Juez apreciará el levantamiento del mismo en atención a las circunstancias del caso".*

El Capítulo IX sobre "Disposiciones Transitorias", se refiere a que las bases de datos deberán adecuarse a la presente ley dentro del plazo de un año de su entrada en vigor.

En el siguiente cuadro se muestran los países latinoamericanos analizados y se señala la fecha de la última legislación en materia de protección de datos del respectivo país, si se regulan en esa normativa los denominados derechos ARCO y si existe o no una Autoridad de Control en materia de protección de datos.

Cuadro comparado de legislación en protección de datos y autoridades de control en Latinoamérica

Cuadro N° 2

PAIS	LEY SOBRE PROTECCIÓN DE DATOS VIGENTE	REGULACIÓN DE LOS DERECHOS ARCO	AUTORIDAD DE CONTROL EN PROTECCIÓN DE DATOS
ARGENTINA	Ley N° 25.326 del 2 de noviembre del año 2000.	Regulados en el artículo 6° de la ley N°25.326.	La Ley N° 27.275 del año 2016, crea la Agencia de Acceso a la información Pública que además regula la protección de datos a través de la Dirección de Protección de Datos Personales.
BRASIL	Ley N° 13.709 del 14 de agosto de 2018. Que entraría en vigencia 2 años después de su publicación lo que se posterga para entrar a regir el 3 de mayo de 2021.	Están regulados entre los artículos 17 al 22 de la ley N° 13.709.	El artículo 65 de la ley crea y regula la Autoridad Nacional para la protección de datos personales - ANPD.
CHILE	Ley N° 19.628 sobre protección a la vida privada, que entra en	Están regulados en el Titulo II de la ley 19.628.	No existe Autoridad de Control. Tangencialmente el

	vigor el 28 de agosto de 1999.		Consejo para la Transparencia tiene facultades residuales en materia de protección de datos solo respecto del tratamiento de entidades públicas.
COLOMBIA	Ley Estatutaria N° 1.581 del 17 de octubre del año 2012	Están regulados en el artículo 8° de la ley N° 1.581.	Entre los artículos 19 al 24 de la ley N° 1.581 se regula la Autoridad de Control y sus funciones radicada en la Superintendencia de Industria y Comercio más concretamente en la Delegatura de la Protección de Datos.
COSTA RICA	Ley N° 8.968 del 7 de julio del año 2011 sobre protección de las personas frente a sus datos personales.	El artículo 7 de la ley N° 8.968 los regula.	Entre los artículo 16 al 20 de la ley N° 8.968 se regula la estructura, personal, funciones y presupuesto de la Agencia de Protección de Datos de los Habitantes entidad adscrita el Ministerio de Justicia y Paz.
ECUADOR	Ley Orgánica de Protección de Datos Personales – LOPDP, vigente desde el 26 de mayo del año 2021.	El Capítulo III de la LOPDP se refiere a los derechos, concretamente entre los artículos 12 al 24.	La LOPDP en su Capítulo XII, artículos 75 al 77, regula a la Autoridad de Protección de Datos Personales cuyo titular será el Superintendente de Protección de Datos.
EL SALVADOR	No existe una legislación que regule la protección de datos personales propiamente. La Ley de Acceso a la Información Pública contenida en el Decreto Legislativo N° 534 del 8 de abril de 2011 se refiere a la protección de datos personales.	La ley de Acceso a la Información Pública aborda en el artículo 31 los derechos ARCO.	No existe una Autoridad de Control propiamente tal, el Instituto de Acceso a la Información Pública de manera residual y tangencialmente aborda algunas cuestiones relativas a la protección de datos personales.
GUATEMALA	No existe ley de protección de datos. La ley de Acceso a la Información Pública contenida en el Decreto N° 57 del 2008 en	El Capítulo VI del Título I se refiere al Habeas Data e indirectamente en el artículo 30 de la señalada ley a los derechos ARCO.	No existe Autoridad de Control en Protección de Datos.

	algunas de sus disposiciones se refiere a la protección de datos.		
HONDURAS	No hay legislación sobre protección de datos. La Ley del Instituto de Acceso de Información Pública contenida en el Decreto Legislativo N° 170 del año 2006 regula indirectamente la protección de datos.	La señalada ley regula el Habeas Data e indirectamente se refiere a los derechos ARCO.	No existe Autoridad de Control en Protección de Datos
MEXICO	Existen dos legislaciones de alcance nacional que regulan la protección de datos. La Ley Federal de Protección de Datos Personales en Posesión de Particulares – LFPDPP que entró en vigor el 6 de julio del 2010 y la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados – LGPDPPSO del 26 de enero de 2017.	La LFPDPP regula los derechos ARCO en el artículo 22 del Capítulo III. La LGPDPPSP regula los derechos ARCO en el artículo 43.	Para ambas legislaciones la Autoridad de Control en materia de protección de datos es el Instituto Nacional de Transparencia Acceso a la Información Pública y Protección de Datos Personales – INAI. A él se refiere el artículo 38 de la LFPDPP y el artículo 88 de la LGPDPPSO.
NICARAGUA	Ley de Protección de Datos Personales N° 787 del 21 de mayo del año 2012.	En el Capítulo III se regulan los derechos de los titulares de los datos y entre los artículos 16 al 18 los derechos ARCO. Además el artículo 10 se refiere al derecho al olvido digital.	El Capítulo V regula la Autoridad de Control que es según el artículo 28 de la ley 787 la Dirección de Protección de Datos, entidad adscrita al Ministerio de Hacienda y Crédito Público.
PANAMA	Ley sobre Protección de Datos Personales N° 81 del 29 de marzo de 2019, que comenzó a regir el 30 de marzo de 2021.	El Capítulo II de la ley N° 81 se refiere a los derechos de los titulares de los datos y a los derechos ARCO el artículo 15 incluyendo el derecho a la portabilidad.	La Autoridad de Control es la Autoridad de Transparencia y Accesos a la Información – ANTAI asesorada por el Consejo de Protección de Datos Personales, entidad colegiada de carácter consultivo regulada en el artículo 35 de la ley N° 81
PERÚ	Ley de Protección de Datos Personales - LPDP N° 29.733 del 21 de junio	El Titulo III de la LPDP se refiere a los derechos de los titulares de los	El Titulo VI de la LPDP se refiere a la Autoridad Nacional de Protección

	del año 2011 complementada por el Decreto Legislativo N° 1.353 del año 2017.	datos personales, regulando los derechos ARCO entre los artículos 18 al 25.	de Datos quien será el Ministerio de Justicia y Derechos Humanos a través de la Dirección Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales. El artículo 33 se refiere a sus funciones y el artículo 36 a los recursos con los que contará.
REPÚBLICA DOMINICANA	Ley N° 172 – 13 publicada el 15 de diciembre del año 2013.	Entre los artículos 7 al 28 se regulan los derechos de los titulares de los datos y también los denominados derechos ARCO.	El artículo 29 de la ley N° 172 hace referencia al órgano de control en materias solamente referidas a cuestiones crediticias, que es la Superintendencia de Bancos, por lo que no existe una Autoridad de Control propiamente tal en materia de protección de datos.
URUGUAY	Ley N° 18.331 sobre Protección de Datos Personales y Habeas Data, del 18 de agosto del año 2018.	El Capítulo III de la ley 18.331 se refiere a los derechos de los titulares de los datos, al derecho de acceso en el art. 14, supresión en el art. 15, impugnación art. 16 y derecho a la comunicación de los datos en el art. 17.	El Capítulo VII se refiere al Órgano de Control que según el artículo 31 de la ley es la Unidad Reguladora y de Control de Datos Personales dependiente de la Agencia para el Desarrollo del Gobierno de Gestión Electrónica y la Sociedad de la Información y el Conocimiento.

Fuente: elaboración propia.

Consideraciones Finales

1. Si bien los países latinoamericanos han realizado esfuerzos para generar directrices comunes en materia de protección de datos, como los Estándares de la Red Iberoamericana de Protección de Datos o la actualización de los Principios para el tratamiento de datos de carácter personal de la OEA del 9 de abril del año 2021, estas constituyen normas de *soft law* que no son vinculantes para los Estados miembros, son

meras normas programáticas que dependen de la voluntad de los legisladores nacionales.

2. El modelo estadounidense de protección de datos personales, choca con la normativa europea lo que ha motivado dos acuerdos que se han demostrado insuficientes como han sido el *Safe Harbour* y el *Privacy Shield*, este último anulado por el TJUE. La regulación norteamericana de la Cloud Act planteará más tensiones entre los dos sistemas normativos. Es cierto que se aprecia una aproximación a la legislación europea principalmente al RGPD en la regulación de la protección de datos del Estado de California, -Ley de Privacidad del Consumidor de California o *California Consumer Privacy Act* o CCPA-, que entró en vigor el primero de enero del año 2020. En esta norma se aprecia el interés comercial de la protección de datos personales, de ahí que se cite a los consumidores, cuando la protección de datos va más allá de las relaciones comerciales.

3. A nivel latinoamericano si bien existe una creciente regulación en materia de protección de datos a nivel constitucional, por ejemplo en la constitución ecuatoriana o a través de leyes de reforma constitucional como es el caso de las Cartas Políticas de México y Brasil, todavía algunas confunden el derecho a la protección de datos con la acción de tutela o garantía denominada habeas data.

4. De las legislaciones de protección de datos revisadas, cualquiera sea el orden o estructura en que se configuren, Títulos, Capítulos o Secciones, en general se distinguen como elementos centrales: una conceptualización de términos en donde destacan las definiciones de datos personales y datos sensibles; los principios en que debe sustentarse el tratamiento de datos; los derechos de los titulares de los datos; la regulación de la transferencia de datos internacional; la autoridad de control en la materia; y la acción o procedimiento de tutela, así como las sanciones a que se verán expuestas las entidades públicas y privadas que no cumplan con sus disposiciones.

5. También destaca en algunas legislaciones latinoamericanas, como la costarricense y mexicana, la referencia que se hace a la autodeterminación informativa, más que a la protección de datos personales, lo que refuerza la dimensión positiva de este derecho que permite al titular disponer, controlar y perseguir su data e información.

6. De igual forma, si bien hay países que no tienen una legislación específica en materia de protección de datos, como es el caso de El Salvador, Honduras o Guatemala, es la legislación sobre transparencia y acceso a la información pública la que regula aspectos relacionados con la protección de datos.

7. Destacable es también que Argentina y Uruguay sean, hasta ahora, los únicos países reconocidos por la Comisión Europea con estándares adecuados en materia de protección de datos personales a efectos de autorización para el flujo transfronterizo de datos personales.

8. A nivel latinoamericano, México aparece con una robusta legislación en protección de datos, regulando tanto el tratamiento que de estos hacen tanto organismos públicos que se denomina sujetos obligados, como instituciones privadas.

9. También en México, resulta llamativo que el consentimiento del titular de los datos, en determinadas circunstancias, pueda ser tácito, salvo en el caso del tratamiento de los denominados datos sensibles, en que siempre deberá ser expreso.

10. El RGPD ha influenciado fuertemente las legislaciones de Latinoamérica en especial las más recientes, como es el caso de las leyes de protección de datos panameña y ecuatoriana, que entraron en vigor a partir del año 2021, o la legislación brasilera en la materia, cuyo articulado completo entró en vigor en agosto del año 2021. En este mismo sentido, la legislación brasilera y ecuatoriana consagran el derecho a la portabilidad de los datos, el cual no está incluido en las legislaciones anteriores que en general solo se refieren a los tradicionales derechos de acceso, rectificación, cancelación y oposición.

11. Por último, no todos los países de la región cuentan con autoridades de control independientes y radican la regulación y promoción de la protección de datos en autoridades administrativas vinculadas a ministerios, como es el caso del Perú, a través del Ministerio de Justicia y en Nicaragua, donde la regulación de la protección de datos está a cargo del Ministerio de Hacienda.

CAPÍTULO IV

LA AUTORIDAD DE CONTROL PARA LA PROTECCIÓN DE DATOS Y SU INDEPENDENCIA

Como se señaló en el capítulo II, los sistemas de garantía de los derechos fundamentales en general distinguen tres categorizaciones: el reconocimiento constitucional, el establecimiento de procedimientos administrativos y jurisdiccionales de tutela y, la generación de entidades u organismos de control y promoción de tales derechos. Hay autores que plantean que las garantías institucionales de los derechos fundamentales pueden entenderse como todos aquellos mecanismos de protección y tutela de los derechos, encomendados a órganos institucionales como el gobierno, el legislador, la administración o los jueces[450].

En este capítulo se abordará este último punto: el mecanismo institucional por medio del cual el ordenamiento jurídico crea órganos autónomos e independientes para velar y promover los derechos y las libertades fundamentales, en este caso la protección de datos personales. Institución inexistente en el sistema chileno y que representa una de las mayores debilidades para la promoción, regulación y control de la protección de datos personales y, que como veremos ha tenido un prolífico desarrollo en Europa e incluso en algunos países latinoamericanos que cuentan con agencias o autoridades de control en la materia[451].

Es que la ausencia de una Autoridad u órgano de control independiente en materia de protección de datos es uno de los principales déficit en el sistema, así lo diagnostica de manera casi transversal la doctrina chilena al señalar "una de las mayores debilidades del régimen de protección de datos radica en carecer de instrumentos jurídicos (recursos o acciones) de defensa agiles y expeditos, sanciones claras a los infractores, así como de una autoridad especializada que se aboque a garantizar su buen funcionamiento y que cautele oportunamente los abusos en el tratamiento de datos y los pueda sancionar oportunamente[452].

A lo largo de la obra empleamos indistintamente la expresión Órgano o Autoridad de Control -que es la terminología empleada en el RGPD, comúnmente aceptada - y Agencias de Protección de Datos que es la expresión empleada en España. Con independencia de su denominación se trata de entidades de carácter público cuya finalidad es vigilar la aplicación de las normas de protección de datos y, por tanto, de que se cumpla la protección de datos con una serie de atribuciones consultivas, investigativas e interventivas[453].

---

[450] Aparicio Wilhelmi M. y Pisarello Prados G. (2013) "Los derechos humanos y sus garantías: nociones básicas". Universitat Oberta de Catalunya, pp.16-17.

[451] Cerda A. (2003). "La autoridad de control en la legislación sobre protección frente al tratamiento de datos perdsonales". Santiago, Tesis para optar al grado de magister en Derecho Público, Universidad de Chile.

[452] Camacho G (2014) La protección de datos como frontera del derecho de acceso a la información". Revista de Grestión Pública, vol. III. N°1, pp.73-93, p.81.

[453] Anguita Ramírez, P. (2007) *"La protección de datos personales y el derecho a la vida privada. Régimen Jurídico, Jurisprudencia y Derecho Comparado"*. Editorial Jurídica de Chile. Santiago de Chile pp 71-72

El sistema europeo de protección de datos presenta dos notas identificativas: una primera, la construcción de un derecho fundamental[454]diferente de la intimidad, honor o privacidad que recibe el nombre de derecho a la protección de datos personales y; la segunda que ahora afrontamos y que constituye el núcleo de esta investigación: el desarrollo de autoridades de control encargadas de vigilar el cumplimento de dicho derecho, aunque como veremos más adelante las competencias van más allá, incluyendo la promoción del derecho o la coordinación con otros organismos, tanto de los encargados de la protección de datos, como de la transparencia.

El primer asunto a abordar será la necesaria independencia de las autoridades de control de la protección de datos, trayendo a colación los principios de la OCDE para mejores prácticas de las agencias independientes. A continuación se revisará como se regula en Europa las autoridades de control inicialmente en la Directiva 95/46/CE y posteriormente en el Reglamento General de Protección de Datos Personales 2016/679 RGPD. Esta norma sirve de referencia en lo relativo al establecimiento y regulación de las autoridades de control, por lo que afrontaremos la independencia de ellas a través de sus competencias, funciones y poderes, con una referencia explícita al flujo transfronterizo de datos personales. Luego, se analizará la configuración de las agencias de control en materia de protección de datos tanto en el contexto europeo como latinoamericano, revisando también la situación de los países de la OCDE y las características que estas instituciones tienen en su conformación, es decir, si asumen exclusivamente la protección de datos o además conjuntamente regulan el acceso a la información pública y la transparencia; si son unipersonales o colegidas, si son autónomas o independientes o dependen de algún ministerio u otra entidad pública, o si tienen reconocimiento constitucional o legal, entre otras consideraciones. A continuación, se analizarán las reformulaciones que la Ley 3/2018 sobre Protección de Datos y Garantías de Derechos Digitales, LOPDGDD, ha realizado sobre la estructura y funcionamiento de la Agencia Española de Protección de Datos.

La Independencia en las Autoridades de Control

Como ya se ha dicho la autonomía o independencia de la Autoridad de Control en la protección de datos personales es un elemento esencial en la configuración del mismo. Esta independencia, ha señalado, la doctrina es posible de entenderla como aquella de la que gozan organismos públicos "con personalidad jurídica propia y plena capacidad de obrar (puede

[454] Como ya se ha señalado en los capítulos anteriores, la protección de datos constituye un derecho fundamental, lo que ha sido reconocido por diversos organismos e instrumentos internacionales. Por ejemplo, la Asamblea General de las Naciones Unidas adoptó la Resolución A/C.3/71/L.39 (2016), sobre derecho a la privacidad en la era digital, en la que exhorta a Estados y empresas a cumplir su obligación de respetar los derechos humanos, especialmente el derecho a la privacidad en la era digital. De igual forma como ya se señaló, en el contexto europeo, el derecho a la protección de datos personales fue objeto del Convenio 108 de 1981 del Consejo de Europa, el primer instrumento internacional que tuvo como finalidad garantizar a cualquier persona física "su derecho a la vida privada, con respecto al tratamiento automatizado de los datos de carácter personal". Asimismo, ha sido reconocido, como derecho fundamental autónomo, en el Artículo 8.1 de la Carta de los Derechos Fundamentales de la Unión Europea, adoptada en el año 2000 y vinculante desde el 2009 como el derecho de toda persona "a la protección de los datos de carácter personal que le conciernan".

contratar por si, tanto públicamente como privadamente) que opera como un órgano de supervisión y control para garantizar la correcta aplicación de la ley"[455].

La OCDE[456] en el estudio sobre el diseño de autoridades reguladoras independientes y responsables de alta calidad distingue cuatro modelos de órganos o autoridades; "(i) Departamentos ministeriales: son órganos que forman parte del gobierno central y no tienen el status de un órgano separado, están dirigidos por o se reportan directamente a un Ministro del Ejecutivo, su financiamiento proviene en gran parte de rentas generales y son parte del servicio civil. Pueden tener algún grado de independencia legal al llevar a cabo funciones regulatorias y también pueden tener una autonomía administrativa considerable de los Ministros; (ii) Agencias ministeriales: son órganos del ejecutivo establecidos fuera del alcance del gobierno central, que pueden o no tener un presupuesto separado y una gestión autónoma. Pueden estar sujetos a diferentes marcos legales (las regulaciones del servicio civil podrían no aplicarse), pueden tener algún tipo de potestad, pero, en definitiva, están subordinadas a un Ministro y sujetas a la intervención ministerial; (iii) Órganos consultivos independientes: son agencias con el poder de proveer asesoría oficial y experta al gobierno, legisladores y empresas en regulaciones y aspectos específicos de una industria. La agencia puede tener la potestad de publicar sus recomendaciones. La posibilidad de que las decisiones públicas se aparten de la recomendación entregada por este órgano puede variar considerablemente; y (iv) Agencias Reguladoras Independientes (ARI): son órganos públicos facultados para hacerse cargo de los aspectos regulatorios de una industria. Generalmente poseen autonomía de gestión, aunque su presupuesto esté bajo el de un Ministerio, sin embargo, no existe espacio para la intervención política o ministerial en ellos, o bien la intervención está limitada a proveer consejo en asuntos generales de política pública y no en casos específicos. Estos órganos tienen potestades que varían entre los diferentes países".

También se puede considerar que estas ARI controlan y tutelan un interés público prevalente, como por ejemplo la infraestructura pública o el medio ambiente, en algunos casos éstas prestaciones que si bien son de interés público, están entregadas a privados, siendo éstas agencias encargadas de regular a dicho privado en el otorgamiento de esa prestación.

Si bien son las ARI las entidades predominantes en la OCDE, no todos los países del bloque se han inclinado por este diseño considerando las complejidades de sus estructuras estatales, en efecto, la independencia de las autoridades regulatorias frente a los ministerios puede ser débil y pueden carecer de los recursos apropiados. Los reguladores son en teoría los que hacen cumplir las leyes (*rule enforcers*), aplican sanciones a quienes no cumplen con las reglas existentes en sus ámbitos de competencia, y autorizan la emisión de licencias y permisos. Sin embargo, la diferencia entre diseñar políticas públicas y regular no siempre es clara: la línea se torna difusa entre la generación de normas (*rule making)* y el hacer cumplir las normas (*rule enforcement*). Es por ello por lo que se establecen mecanismos de accountability. Un marco claro para la existencia de regulación de alta calidad es también imprescindible para garantizar

[455] Sanchez de Diego Fernandez de la Riva, M. (2022), "El derecho de acceso a la información pública. Un tortuoso camino. O como convertir la carretera de la transparencia en una autopista", Editorial Fragua, Madird, pp. 365 – 369.

[456] OCDE (2005) "*Designing Independent and Accountable Regulatory Authorities for High Quality Regulation, Working Party on Regulatory Management Reform*" http://www.oecd.org/regreform/regulatory-policy/35028836.pdf

transparencia, predictibilidad y eficiencia en marcos regulatorios promercado que exijan el cumplimiento normativo.

Los reguladores independientes representan un aspecto clave de la gobernanza moderna. En efecto, como se sostiene por parte de la OCDE, las entidades regulatorias forman parte importante del quehacer estatal pero se diferencian de las funciones asociadas a la propiedad del Estado y de la formulación de políticas públicas. La racionalidad que subyace al establecimiento de agencias regulatorias independientes consiste en asegurar que las decisiones que afectan a sectores fundamentales de la infraestructura y economía de un país queden protegidas de las consideraciones políticas de corto plazo y de los grupos de interés privados. Los reguladores independientes son utilizados cuando se establecen nuevos marcos regulatorios promercado en servicios públicos, en las telecomunicaciones, en los servicios financieros, o en otros sectores sociales o medioambientales.

Desde la perspectiva de la gobernanza pública, estos reguladores son "agencias" a las que se les han confiado poderes regulatorios significativos y a los que se les ha conferido un cierto nivel de independencia en su proceso de toma de decisiones: mientras las agencias tradicionales todavía responden frente al Ejecutivo, incluso cuando se les ha conferido un nivel alto de autonomía operacional y presupuestaria, estos reguladores se estructuran organizacionalmente potenciando su independencia.

Ellos pertenecen a un sistema de "pesos y contrapesos", diseñado para equiparar el poder de los Ministros del Ejecutivo y los grupos de interés. Finalmente, la OCDE destaca que las autoridades regulatorias independientes han sido establecidas bajo diferentes regímenes incluyendo sistemas parlamentarios y presidenciales. De igual forma el poder o facultades que se deleguen en las autoridades regulatorias, dependerá también de aspectos históricos y culturales y del marco constitucional en el que éstos se desarrollen.

La profesora María Salvador Martínez ha estudiado las "Autoridades Independientes"[457] señalando las garantías relacionadas con las mismas: autonomía orgánica, autonomía financiera, autonomía funcional y autonomía personal.

La autonomía orgánica supone que el órgano administrativo se crea por ley, se reconoce su personalidad jurídica propia y se le permite aprobar sus propios estatutos o reglamentos internos. La autonomía financiera implica el control de sus recursos económicos, tanto de los propios como de los públicos. La autonomía funcional, que reside en primer lugar en el desempeño de sus funciones, lo que implica que los titulares de estas agencias ni tampoco ninguno de los servidores públicos a su servicio pueden recibir recomendaciones, instrucciones u órdenes de órganos privados o públicos. La autonomía personal garantiza la independencia a partir de un procedimiento de elección en el que se busque la idoneidad de su titular y de los servidores públicos que en esa entidad se desempeñen, a lo que se agrega el procedimiento de destitución que ha de estar tasado por causas objetivas y no debería dejarse al libre albedrío del Gobierno[458].

---

[457] Salvador Martínez, M. (2002): *"Autoridades Independientes"* Ariel, Barcelona, 2002.

[458] Sanchez de Diego Fernandez de la Riva, M. (2022), "El derecho de acceso a la información pública. Un tortuoso camino. O como convertir la carretera de la transparencia en una autopista", Editorial Fragua, Madird pp. 365 – 369.

Conviene señalar que en el ordenamiento jurídico chileno el concepto de autonomía tiene diversos alcances, como señala Cordero Quinzacara; "Así, nuestra Constitución habla de la autonomía de los grupos intermedios o de la autonomía municipal, del Banco Central y de diversos órganos que integran la Administración del Estado. En este caso en particular, es importante distinguir entre autonomía política y autonomía administrativa, conceptos que muchas veces se confunden y que corresponden a diversos niveles o etapas en la organización del Estado. La autonomía política se predica de aquellos Estados compuestos, en donde el poder político no sólo es distribuido a nivel horizontal (poder legislativo, judicial y ejecutivo), sino también de forma vertical: Estado federal y Estados federados, Estado central y regiones. Son casos que también se comprenden bajo la noción de descentralización política, ya que existe más de un centro de impulsión del poder, como ocurre con los Estados federales o regionales, en donde se comparte el poder legislativo a nivel central o federal y a nivel de estados miembros o regiones; lo mismo que el gobierno.

Distinto es el caso de la autonomía administrativa, pues ésta no supone necesariamente la existencia de descentralización política. La autonomía administrativa supone la existencia de órganos que forman parte de la Administración del Estado, pero cuya relación con el poder central o las máximas autoridades gubernativas es tenue o casi inexistente, lo cual le permite actuar con independencia al momento de adoptar sus propias decisiones. En muchos de estos casos, la entidad autónoma goza de personalidad jurídica y patrimonio propio, pero no es una condición esencial, tal como lo explicaremos más adelante. Ahora bien, conforme a nuestra Constitución, no es posible la existencia de órganos, entidades o regiones que gocen de autonomía política, ya que esto supone una descentralización política que no se condice con el carácter unitario que le asigna la Carta Fundamental a nuestro Estado (artículo 3º). Sin embargo, lo anterior no es óbice para que dentro de la Administración del Estado puedan existir órganos autónomos de naturaleza administrativa, como da cuenta la propia Carta Fundamental: Contraloría General de la República, Banco Central, Municipalidades, Consejo Nacional de Televisión. Además, también se permite al legislador crear órganos de la misma naturaleza (artículo 65 inciso 4º Nº 2)" [459].

Bajo el término "agencias independientes" los autores hacen referencia a aquellos organismos públicos inmersos en la estructura de la Administración del Estado, creados en tal condición o bien reformados hacia esa figura y que disponen de una importante autonomía frente al Gobierno y específicamente al poder del Presidente de la República, siendo competentes para actuar en diversos ámbitos tales como la economía, la política y la problemática social, sin mayor ligazón o vínculo con la administración centralizada o si se quiere con el núcleo o centro de poder[460].

Estas agencias entonces gozan de un considerable nivel de autonomía o independencia asignado por la Constitución o las leyes para el desempeño de su función, teniendo mayor libertad para el ejercicio de sus actuaciones que las que tradicionalmente tienen los

[459]Cordero Quinzacara, E. (2012), "La Admnistración del Estado en Chile", en "*La Contraloría General de la República, 85 años de vida institucional* (1927-2012)", ediciones Contraloría General de la República, Santiago de Chile, ciudad, pp.15-34.

[460] Salvador Martínez, M.. (2002), *"Autoridades independientes"*, Ariel Derecho, Madrid. p. 29.

denominados órganos autónomos descentralizados[461], de ahí entonces que la literatura prefiera la denominación "órgano independiente"[462].

En síntesis, como señala Salvador Martínez, son organizaciones de carácter institucional, no representativas, que desarrollan funciones propias de la Administración activa y que están configuradas legalmente de forma que el Gobierno y el resto de la Administración gubernativa carecen de las facultades de dirección que configuran típicamente su relación con la Administración institucional instrumental, con la finalidad de neutralizar políticamente una actividad integrada en la órbita del Poder Ejecutivo.[463]

En el derecho comparado, admiten diferentes denominaciones; en Reino Unido se les ha dado el nombre de *quangos o quasi autonomous non governmental organisations,* en Estados Unidos, *independent agencies*, en Francia se les denomina *autorités administratives indépendantes*; en Alemania, *funktionale Selbstverwaltungsträgern*; en España, autoridades independientes. Cualquiera sea su denominación, estas entidades independientes han sido estructuradas sobre la base de disponer de un régimen mayor de independencia del poder central que aquella sobre la cual fueron diseñadas las denominadas "instituciones descentralizadas".

Elementos de las entidades independientes

Por regla general los elementos que constituyen a las entidades independientes son fundamentalmente tres[464]:

1. La neutralidad política: supone que ciertas funciones se ejerzan al margen de la dialéctica política partidista. Se requiere alejar determinadas actividades y decisiones del ámbito de influencia de los partidos políticos y, más concretamente, de los órganos del Estado en los que tiene lugar esa controversia. Lo que se busca es garantizar una cierta "neutralidad" o "imparcialidad" en el ejercicio de la función y para ello es preciso atribuir dicha función a un organismo "alejado" (independiente) de los órganos políticos del Estado.

2. La especialización técnica: este tipo de agencias deben adoptar decisiones de alto contenido técnico que pueda superar la trampa de la denominada inconsistencia dinámica, es decir, que se confundan las prioridades técnicas de corto y largo plazo. Se afirma que la "independencia" permitiría sustraer al Gobierno de turno de adoptar decisiones que afecten los objetivos técnicos de una regulación consistente en el largo plazo.

---

[461] En la descentralización administrativa en general es posible distinguir tres elementos; personalidad jurídica propia, patrimonio propio y tutela atenuada o supervigilancia del Presidente de la República, que se relaciona con dichos órganos a través del respectivo ministro de Estado.

[462] Salvador Martínez, op. cit. P. 344 - 350.

[463] Magide Herrero, M. (2000), "Límites constitucionales de las Administraciones independientes, (MAP-INAP)", editorial, ciudad, p. 33.

[464] Salvador Martínez, op. cit., p. 344 – 350.

3. La eficacia: considerando que estas agencias se separan de la política y responden a objetivos técnicos, deben estar afectas a un régimen jurídico que les permita funcionar con oportunidad adecuada para resolver los problemas que les han sido entregados por la ley. Por tal motivo, los sistemas legales han tratado de diseñar distintas fórmulas para generar esa denominada independencia. Los elementos que particularizan a las agencias independientes según la literatura son[465]: (a) el elemento funcional, que implica excluirlas de las directivas gubernativas y los recursos jerárquicos y dotarla de potestades normativas independientes; (b) el elemento humano o de personal, que supone establecer mecanismos independientes de designación y mandato de los titulares de los órganos rectores de su administración, lo cual supone restricción en la remoción y disponer de garantías que eviten la "captura" por parte de algunos administrados; y (c) elementos complementarios tales como idoneidad de la organización administrativa y medios financieros de limitación restringida.

Lo que se persigue es que las decisiones sean adoptadas con prescindencia de las preferencias coyunturales de un Gobierno determinado, permitiendo sostener una política pública consistente en el largo y en el corto plazo[466]. Siendo una de las manifestaciones más evidentes de aquello, más que el reconocimiento constitucional de la autonomía, la manera en que son generadas sus autoridades superiores, así como, especialmente, su régimen de remoción, incompatibilidades y dedicación.

Estabilidad versus Legitimidad y Tecnicismo versus Armonía, como elementos de la Independencia

Diversos estudios[467] dan cuenta sobre la configuración de agencias regulatorias independientes, los que son posibles de abordar desde dos perspectivas que influyen en su independencia, distinguiendo entre: a) estabilidad-legitimidad y b) tecnicismo-armonía. La primera, estabilidad versus legitimidad, implica que la independencia otorga estabilidad a las directrices que regulan un determinado sector, sobre todo cuando existen contextos de polarización o controversia política sobre la regulación de un determinado sector, la independencia se constituye entonces como un instrumento de restricciones recíprocas donde los actores en disputa convergen hacia un determinado consenso. Esto es lo que se denomina el "principio del aliado", donde entre el gobierno y las agencias reguladoras existe una cercanía o afinidad ideológica, lo que le permite al primero restringir o ampliar el ámbito de actuación de la segunda. Dado que los cambios de gobiernos son decisivos para la gestión de la agencia,

[465] Ver García, J. F. y Verdugo, S. (2010), "De las Superintendencias a las Agencias Regulatorias Independientes en Chile: Aspectos Constitucionales y de Diseño Regulatorio", *Actualidad Jurídica Universidad del Desarrollo*, vol. XXII, pp. 263-305.; Rajevic, E. (2010), "El Consejo para la Transparencia como Agencia Independiente", en Varios Autores (edit.) "*Transparencia en la Administración Pública"*, Santiago, Abeledo Perrot, pp. 231-247.

[466] Ibídem.

[467] Pardow, D. (2018), "¿Técnicos o políticos?: Radiografía del Sistema de Nombramiento de Directores de Agencias Regulatorias Independientes", *Revista Chilena de Derecho*, Vol. 45, N°3, pp.745-769.

por consiguiente, la independencia es un elemento que morigera el cambio gubernamental[468]. En definitiva, con la independencia se limita el poder del ejecutivo para formular e implementar solo políticas públicas de su preferencia.

Así, por ejemplo, para la designación de un directivo público, en el caso que nos ocupa de la Autoridad de Control en materia de protección de datos, la confirmación del parlamento produce en el postulante de la coalición gobernante la necesidad de convencer a toda o al menos una parte de la coalición opositora, para que concurra en la aprobación de su designación, generando una mayor moderación en sus planteamientos y propuestas. Lo anterior limita la posibilidad del ejecutivo de utilizar las designaciones o remociones como un incentivo para influir en la gestión y decisiones que adopte la agencia. Como contrapartida, como se sabe, el gobierno es electo democráticamente y los directivos de las agencias independientes no, por lo que limitar al ejecutivo para designar a sus directivos puede afectar la legitimidad de estos.

Desde otra perspectiva, las designaciones pueden hacerse sirviéndose de una mayoría circunstancial que afecte a sucesivos gobiernos, impidiendo cambios regulatorios más profundos, esto es lo que se ha denominado la dinámica del "atrincheramiento". Un ejemplo de ello es lo que ocurrió en EE. UU con la Comisión Interestatal de Comercio o *Interstate Commission of Commerce*, creada en 1887, donde la ley creaba la agencia y disponía que para la designación de su cuerpo directivo se requería la aprobación por mayoría del saliente Partido Demócrata, después de que este perdiera las elecciones y pocos meses antes de que la entrante mayoría del Partido Republicano asumiera sus funciones. Lo que se buscaba era limitar la capacidad del gobierno entrante para cambiar la regulación, ya que los demócratas apoyaban la fijación de precios y los republicanos la libertad tarifaria[469].

Así entonces, definir cuánta independencia resulta óptima, exige ponderar los valores opuestos de estabilidad y legitimidad. Sobre el tecnicismo versus la armonía, lo primero es señalar que en muchas ocasiones los mecanismos de independencia formal se abordan como herramientas para mejorar la calidad de las decisiones regulatorias[470]. Así, en las designaciones o nombramiento de los directivos de agencias reguladoras, la dinámica de frenos y contrapesos implican que quien comienza con el proceso de selección debe convencer a otros organismos del Estado respecto de las virtudes de los candidatos que presenta, lo que genera incentivos para buscar personas cuya capacidad técnica se vea reflejada en la formación académica, experiencia profesional, y otros antecedentes objetivos. A su vez, el limitar la remoción discrecional de los directivos de una agencia permite que las decisiones regulatorias sean adoptadas sin temor a represalias. Dicho de otro modo, la independencia persigue que las designaciones se sustenten en la competencia técnica del postulante y no en su preferencia o afiliación política. El objetivo es que quien debe realizar la designación, es decir, el ejecutivo,

[468] Levy B. & Spiller, P. (1996), "*Regulations, Institutions and Commitment"*, New York, Cambridge University Press.

[469] Wood, D. & Bothe, J. (2004), "Political transaction costs and the politics of administrative design", *Journal of Politics*, Vol. LXVI, N° 1, pp. 176–202.

[470] Bawn, K. (1995), "Political control versus expertise: Congressional choices about administrative procedures", *American Political Science Review*, Vol. LXXXIX, N° 1, pp. 62-73.

no solo busque satisfacer sus propios intereses, que es lo que se denomina la selección adversa o tenga que optarse entre profesionalizar y burocratizar[471].

Sin menospreciar las ventajas del tecnicismo, es evidente que este también genera complejidades, en efecto, se hace más difícil verificar el cumplimiento de los objetivos institucionales, ampliando así el espacio de discrecionalidad efectiva con que la agencia toma decisiones[472]. Mientras mayor es la especificidad técnica de la regulación, se incrementan también las asimetrías de información entre la agencia regulatoria y los órganos de representación política. Por otra parte, fomentar la responsabilidad individual de una agencia, lógicamente disminuye sus incentivos para colaborar con otros potenciales organismos involucrados. Cuando son los directivos quienes reciben directamente los castigos y recompensas, el proceso de toma de decisiones regulatorias pasa a estar gobernado por el interés particular de la agencia y no por el bienestar social[473].

Como se puede advertir, la independencia en la designación de los directivos de agencias reguladoras o de una Autoridad de Control para la protección de datos personales no es solo un objetivo en sí mismo, si no que invita a preguntarse qué tipo de regulación se quiere y para qué. Si bien la experiencia comparada muestra que el carácter independiente de la autoridad de control es mayoritario, no necesariamente es expresión de una mejor regulación o calidad de las políticas públicas que formule e implemente. Sin embargo, disminuir la influencia de los gobiernos de turno en las instancias de designación de sus directivos permite promover liderazgos estables y técnicos, lo que resulta fundamental, en especial si el espacio de regulación dice relación con un derecho fundamental, en este caso, el de la protección de datos de carácter personal, así lo demuestra la experiencia empírica.[474]

En definitiva, la independencia altera la verticalidad y jerarquía que caracteriza al Poder Ejecutivo, incrementar la independencia institucional es también una manera de generar visibilidad, esto es, facilitar que los responsables de la agencia reciban crédito por sus aciertos y se hagan responsables de sus errores. Teniendo en cuenta que ejercer apropiadamente la función regulatoria toma tiempo y esfuerzo, la independencia funciona como una manera de recompensar a los reguladores por hacer bien su trabajo[475].

La Responsabilidad de una Autoridad Independiente

La responsabilidad constituye un elemento constitutivo de todo Estado de Derecho, en efecto, todo aquel sujeto que cause un daño o perjuicio deber responder por ello, y el Estado,

---

[471] Wilson, J. (1989), "Bureaucracy: What government agencies do and why they do it", New York, Basic Books.

[472] Gallimard, S. (2002), "Expertise, subversion, and bureaucratic discretion", *Journal of Law, Economics and Organization*, Vol. XVIII, N° 2, pp. 536-555.

[473] Rose-Ackerman, S. (1986), "Reforming public bureaucracy through economic incentives?", *Journal of Law, Economics and Organization*, Vol. II, N° 1, pp. 131-161.

[474] Krause, G. & Meier, K. (edit.) (2003), "Politics, policy, and organizations: Frontiers in the scientific c study of bureaucracy", Michigan, University of Michigan Press.

[475] Stephenson, M. (2007), "Bureaucratic decision costs and endogenous agency expertise", *Journal of Law, Economics and Organization*, Vol. XXIII, N° 2, pp. 469-498.

personificado en distintos organismos, entidades o servicios públicos como sujeto jurídico, si en el ejercicio de su función pública genera un perjuicio también deberá responder.

La responsabilidad del Estado y sus organismos, en este caso de una Autoridad de control independiente, para la regulación y promoción de la protección de datos de carácter personal se encuentra vinculada a la necesidad de establecer mecanismos de confianza hacia los ciudadanos y también de garantía frente a sus actuaciones. Como ha señalado la doctrina el fundamento histórico, político y administrativo de la responsabilidad radica en su configuración como garantía jurídica de los administrados frente al Poder Público, y consiguientemente, vinculada en su esencia a una forma de resarcimiento de los particulares frente a eventuales efectos lesivos derivados de la acción administrativa[476].

La Administración Pública bajo cualquier fórmula de personificación, en este caso como una Autoridad de Control en materia de protección de datos no es un sujeto cualquiera, es una institución reconocida por la Constitución y las leyes compuesta por privilegios y limitaciones: en el sistema jurídico-administrativo continental, cuando unos dañan a otros, los unos compensan a los otros. Los privilegios se les confieren por que la Administración actúa fiduciariamente, en persecución de un interés general, en este caso tutela los datos e información de sus titulares, para que estos puedan resguardar, controlar y perseguir la información que les es propia. Las limitaciones que se impongan a una Autoridad de Control y a cualquier otro órgano de la administración, buscan garantizar que no se desvíen de este fin y para que cuando actúe respete los derechos y libertades de los ciudadanos.

El cómputo de potestades y limitaciones sobre su ejercicio, que se recoge en normas constitucionales y legales configura un régimen jurídico específico, una subordinación integrada en el sistema jurídico general del Estado. Y es en ese contexto en el que debe interpretarse la responsabilidad de la administración[477], en este caso de una Autoridad de Control independiente en materia de protección de datos.

Si bien no es parte de la presente investigación abordar el régimen de responsabilidad de la Autoridad de Control en materia de protección de datos, es pertinente remarcar que su naturaleza autónoma o independiente no la excluye de la responsabilidad a la que están afectos todos los órganos de la administración del Estado y principalmente esbozar aquí para luego desarrollar en el capítulo final de este trabajo algunos elementos relacionados con la responsabilidad o más bien con la rendición de cuentas que una entidad de esta naturaleza debería asumir. En efecto, en términos generales se propone un régimen de rendición o de cuentas asociado al ejercicio de sus atribuciones que considere tres perspectivas: a) La económica: que considere su patrimonio, para los efectos de que se ejecute adecuadamente su presupuesto y que sus funcionarios o personal dependiente que tenga a su cargo o administre recursos fiscales rinda cuenta de su ejercicio; b) La política, para que de manera regular y

[476] Dadingo Guerra, A. (1996) " Sobre la aplicación extensiva de la institución de la responsabilidad patrimonial de la Administración a los daños sufridos por entidades públicas". Revista Española de Derecho Administrativo REDA, N° 92, p. 652.

[477] Gamero Casado, E. (1997) "Las transformaciones del sistema de responsabilidad administrativa extracontractual". En *La responsabilidad patrimonial de los poderes públicos en el marco de la estructura territorial del Estado. III Jornadas d eestudio del Gabinte Jurídico de la Junta de Andalucia*. Granada: Comares.

periódica, por ejemplo anualmente, dé cuenta de su gestión ante el Congreso o Parlamento del respectivo Estado a través de una cuenta pública que este contenida en un informe de gestión que incluya los procedimientos administrativos sustanciados para tutelar la protección de datos y el resultado y estadísticas de los mismos; y finalmente c) La Jurídica, por cuanto todas la actuaciones de la Autoridad de Control contenidas en sus pronunciamientos o resoluciones serán susceptibles de ser impugnadas por la vía judicial ante los tribunales de justicia.

Como señala María José Blanco Antón "La independencia de las autoridades de control no debe significar que dichas autoridades puedan quedar exentas de mecanismos de control o supervisión en relación con sus gastos financieros, o de control judicial. Para ello, y sin perjuicio de las competencias del Tribunal de Cuentas, la gestión económico financiera de la Agencia se encuentra sometida al control de la Intervención General de la Administración del Estado en los términos que establece la Ley 47/2003, de 26 de noviembre, General Presupuestaria"[478].

Principios OCDE para mejores prácticas de las agencias independientes

La OCDE[479] ha establecido siete principios sobre mejores prácticas para la Gobernanza de los Reguladores o agencias independientes, que son lineamientos para fortalecer su diseño institucional y, por tanto, buscan mejorar su desempeño. Estos principios son:

1. Claridad en los roles

La idea principal de este principio es que un regulador eficiente debe tener objetivos y funciones claras, integrados en un marco regulatorio integral y otros instrumentos de política.

---

[478] Blanco Antón, M., (2019), "Autoridades de Control Independientes (Arts. 51-59 RGPD). Autoridades de Protección de Datos (Arts. 44-59 y Disposición adicional cuarta LOPDGDD)", en "*La Adaptación al Nuevo Marco de Protección de Datos tras el RGPD y la LOPDGDD"*, Coordinador José López Calvo, Boch Wolters Kluwer, p. 611.

[479] OCDE (2014) "*Best Practice Principles for Regulatory Policy. The Governance of Regulators*" https://www.oecd-ilibrary.org/the-governance-of-regulators_5jz8qhtck96d.pdf?itemId=%2Fcontent%2Fpublication%2F9789264209015-en&mimeType=pdf El capítulo 3 Decision making and governing body structure for independent regulators (Toma de decisiones y estructura de órganos de gobierno para reguladores independientes) https://www.oecd-ilibrary.org/deliver?redirecturl=http%3A%2F%2Fwww.keepeek.com%2FDigital-Asset-Management%2Foecd%2Fgovernance%2Fthe-governance-of-regulators%2Fchapter-3-decision-making-and-governing-body-structure-for-independent-regulators_9789264209015-8-en&isPreview=true&itemId=%2Fcontent%2Fcomponent%2F9789264209015-8-en OCDE (2014) Best Practice Principles for Regulatory Policy. The Governance of Regulators https://www.oecd-ilibrary.org/the-governance-of-regulators_5jz8qhtck96d.pdf?itemId=%2Fcontent%2Fpublication%2F9789264209015-en&mimeType=pdf El capítulo 3 Decision making and governing body structure for independent regulators (Toma de decisiones y estructura de órganos de gobierno para reguladores independientes) https://www.oecd-ilibrary.org/deliver?redirecturl=http%3A%2F%2Fwww.keepeek.com%2FDigital-Asset-Management%2Foecd%2Fgovernance%2Fthe-governance-of-regulators%2Fchapter-3-decision-making-and-governing-body-structure-for-independent-regulators_9789264209015-8-en&isPreview=true&itemId=%2Fcontent%2Fcomponent%2F9789264209015-8-en consulta efectuada el 24 de junio de 2020.

Estas funciones deben ser suficientes para alcanzar los objetivos institucionales que dieron origen a la creación de los reguladores. La principal justificación de este principio es que solo a través de objetivos e indicaciones claras, la institución puede lograr los resultados y alcanzar las metas esperadas.

Estos objetivos de los reguladores no deben estar en conflicto o competir en las metas, de otra forma ello puede perjudicar el desempeño institucional. Solamente cuando haya beneficios claros que superen los costos potenciales de combinar estos objetivos será adecuado unirlos. Sin embargo, en una situación en que el regulador agrupe objetivos contrapuestos, es esencial desarrollar un marco regulatorio y lineamientos que ayuden a la institución a compensar dichas funciones. Por otra parte, al interior de la institución estos objetivos deben reflejarse en funciones, metas, presupuesto, personal, entre otros elementos, separados y específicos. Por tanto, un regulador de múltiples objetivos enfrentaría retos importantes al planear y ejecutar todas las responsabilidades y funciones.

Este marco legal debe indicar los mecanismos de coordinación por medio de los cuales el regulador debe colaborar con otras instituciones en temas de responsabilidad compartida; por ejemplo, congreso, ministerios, organismos autónomos, etc. Por otro lado, cualquier acuerdo de cooperación, memorándum de entendimiento o acuerdo formal debe ser publicado en las páginas web de los reguladores para promover la transparencia en los roles del regulador.

Una clara separación de funciones y coordinación con los ministerios resulta ser un asunto importante. El papel de los reguladores en relación con su contribución sobre los objetivos de los ministerios puede variar de país a país. Sin embargo, una práctica común es el principio de la independencia de los reguladores, que limitaría la responsabilidad de apoyar a los ministerios en sus objetivos de política pública. No obstante, el apoyo en los asuntos es un hecho y también es deseable la participación de los reguladores en las distintas etapas de la formulación de políticas ya que la coordinación entre la promoción y la regulación reduce la incertidumbre y alinea las expectativas sobre el papel de los entes regulados.

Este primer principio resulta fundamental de considerar en el caso de agencias o autoridades de control que surgieron primero con la función de regular la protección de datos personales y luego se hicieron cargo, conjuntamente con ello, de la regulación del derecho de acceso a la información pública, o a la inversa. Según esta directriz, el desarrollo de funciones y objetivos reguladores nítidos podría desdibujarse si se le adicionan posteriormente otras, distintas a las que originalmente la entidad de control desarrollaba, a menos que exista una adecuada coordinación y estructura organizacional que impida el conflicto o superponga objetivos y metas.

Lo anterior es especialmente relevante si se tiene en cuenta que la protección de datos y el acceso a la información pública son derechos diferentes y en algunos aspectos hasta antagónicos. La protección de datos tiene por objetivo garantizar la información y datos de sus titulares, estando facultados éstos, no solo para impedir la intromisión o tratamiento sobre ellos de parte de un tercero sea público o privado, sino también tiene como objetivo el que sus titulares puedan controlar y perseguir su información. En cambio, el objetivo del acceso a la información pública es evitar la corrupción y fomentar la transparencia de las actividades que desarrollan y de las decisiones que adoptan, así como sus fundamentos.

2. Evitar la influencia indebida y mantener la confianza

Este principio se sustenta en que los reguladores necesitan generar confianza entre los actores involucrados y las instituciones. Con el objeto de crear esta confianza es necesario mantener una comunicación cercana con las entidades reguladas y otras partes interesadas, pero al mismo tiempo el regulador debe mantenerse alejado de cualquier influencia indebida que pudiera generar su captura.

La labor de los reguladores debe basarse en la objetividad y la imparcialidad, por ello, si existe una situación en que el alcance del regulador abarque al gobierno y a las empresas no gubernamentales, se requiere de una neutralidad competitiva para evitar la desconfianza y reducir el riesgo de influencia indebida por parte de empresas públicas.

La independencia formal y real puede promover la objetividad e imparcialidad. Los estatutos jurídicos pueden otorgar independencia legal de los reguladores, en tanto que la independencia puede surgir de la fortaleza institucional o la implementación de mejores prácticas. Ambos esquemas enfrentan ventajas y retos, la selección de una de ellas depende de diversas condiciones, por ejemplo, la necesidad de demostrar independencia, la dinámica de la política a nivel nacional o la fortaleza institucional del país.

La influencia indebida puede surgir de cualquier institución gubernamental (ministerios, congreso, poder ejecutivo, organismos autónomos, poder judicial, entre otros.), los entes regulados o el público en general. El regulador necesita interactuar con estas partes para desplegar el proceso regulatorio, coordinando los temas de responsabilidades compartidas, llevando a cabo consultas sobre los proyectos regulatorios y recibiendo retroalimentación sobre la estrategia y los instrumentos que aplica. Sin embargo, en esta interacción el regulador debe buscar el objetivo institucional en el corto y largo plazo evitando la influencia indebida.

Evitar la captura del regulador y mantener la confianza asegura que los reguladores o agencias independientes de hecho persigan los objetivos que se originaron. Existen diversas prácticas que contribuyen a reducir el riesgo de captura regulatoria y por ende generan confianza, por ejemplo, la restricción de "puertas giratorias" para los funcionarios que laboran en empresas reguladas después de cierto periodo; comunicaciones transparentes entre reguladores y actores involucrados; una agenda definida y canales oficiales de comunicación; el grado de independencia formal y jurídica y el proceso de consulta para la producción regulatoria; el proceso de selección y los periodos en que los directivos o consejeros ejercen sus funciones, entre otras materias.

Los reguladores pueden ser desde órganos ministeriales hasta autónomos. La influencia indebida y los desafíos sobre la confianza son distintos en ambas situaciones. En principio, la influencia podría ser más probable entre los reguladores ministeriales en comparación con los órganos de gobierno, pero aquellos pueden enfrentar los desafíos de forma oportuna y efectiva. La elección entre uno y otro depende de los arreglos y la capacidad institucionales no solo del regulador sino también de los entes públicos.

Así entonces, la autoridad de control debe considerar una doble perspectiva, por un lado, no debe ser influenciada por otras entidades públicas o autoridades de gobierno que en el desempeño de su función también le corresponderá fiscalizar y por otro lado no verse afectada o influenciada por las entidades del sector privado que le corresponderá regular.

La ausencia de una autoridad de control genera desconfianza tanto en los mercados como entre las entidades públicas, por cuanto deja varias respuestas sin contestar; ¿Quién se preocupa de que los contratos que se firman masivamente no violenten la norma de orden público de

caducidad?. ¿Quién promueve campañas de educación sobre la importancia de cuidar los datos personales en las redes sociales? ¿Quién investiga y sanciona las vulneraciones de datos personales? ¿Quién sanciona a las empresas que trafican datos personales de sus clientes?[480].

Este segundo principio adquiere importancia si se tiene en cuenta que la mayoría de las agencias de control en materia de protección de datos regulan el tratamiento de la información que hacen tanto entidades privadas como organismos públicos, considerando que ambos reciben, transfieren y almacenan una enorme cantidad de datos, por lo que en su función de promoción y regulación y con el fin de tutelar el derecho fundamental de proteger los datos de carácter personal no pueden distinguir, salvo las expresas excepciones que se establezcan por ley (por ejemplo razones de defensa o seguridad nacional o por la afectación de otro derecho fundamental), si el tratamiento de datos lo realiza una entidad privada o una institución pública.

3. Toma de decisiones y estructura de órganos de gobierno para reguladores independientes

El diseño del ente gubernamental y las facultades para la toma de decisiones tienen impacto sobre la efectividad de los reguladores, la entrega de la política regulatoria y los resultados esperados sobre los objetivos institucionales. Adicionalmente, el órgano rector tiene influencia sobre la integridad de los reguladores ya que puede afectar el riesgo de caer en captura regulatoria.

El órgano rector del regulador puede tomar distintas formas[481]:

- El modelo de órgano colegido como un consejo o directorio: supervisión, dirección estratégica y política operativa.
- El modelo de comisión: donde la instancia pluripersonal asesora sobre decisiones regulatorias.
- Miembro único: un individuo toma las decisiones regulatorias. Existe una única autoridad reguladora.

La selección del modelo *per se* tiene algunos efectos sobre la efectividad del regulador. Por ejemplo, bajo ciertas condiciones un modelo de comisión o colegiado reduce el riesgo de captura regulatoria y fortalece la toma de decisiones en comparación con el modelo de autoridad única.

La designación del órgano rector debe ser abierta y pública, promoviendo la transparencia evitando la captura regulatoria. Con el objeto de ir en esa dirección es necesario establecer políticas, criterios y procesos de selección preventivos y transparentes. Los miembros del órgano rector pueden ser elegidos por medio de concurso público o por nombramiento directo de una autoridad. Sin embargo, el concurso público brinda mayor confianza si se hace con criterios de selección estandarizados y objetivos.

---

[480] Alvarez Valenzuela, D. (2016), "Acceso a la Información Pública y Protección de Datos Personales. ¿Puede el Consejo para la Transparencia ser la Autoridad de Control en materia de Protección de Datos?", en Revista de Derecho de la Universidad Catolica del Norte. Año 23, N°1, 2016, pp. 51-79.

[481]

La elección directa de la instancia colegiada es otra práctica común de los reguladores. Este tipo de órgano rector puede ser electo por una autoridad o por diferentes funcionarios públicos. No obstante, el modelo requiere más transparencia en los criterios de elección ya que podría existir sesgo en el proceso. Por ejemplo, los representantes de los actores interesados, la industria y el ministerio pueden estar en conflicto con los antecedentes técnicos. Los reguladores deben seguir sus objetivos institucionales pero los miembros pueden estar influenciados o tener opiniones sesgadas debido al cargo público que ocupan. Por ello, se recomienda tener enunciados claros sobre los objetivos y las metas, así como lineamientos que reduzcan el conflicto.

Un modelo basado en un consejo tiene más memoria institucional cuando el reemplazo es escalonado. Debido a esto, los cambios en la instancia colegiada son menos costosos y con menor probabilidad de modificar completamente el trabajo del regulador. Este modelo puede alejar a la institución del proceso político. Por ejemplo, el nombramiento puede ir más allá de los periodos presidenciales o escalonar dicho nombramiento.

Sin menoscabo del modelo de gobierno, en términos generales, los modelos corporativos o colegiados tienen características más flexibles para impulsar la rendición de cuentas, la transparencia, efectividad, integridad e independencia del regulador. En contraste, una autoridad única puede ser más adaptable a los cambios de la industria y su capacidad de respuesta más rápida. La captura regulatoria es más desafiante cuando hay un solo miembro, pero la fortaleza institucional del ministerio principal puede brindar su apoyo en este asunto.

Como ya se analizará, en la experiencia comparada no existe un sistema preferente para la instalación de una autoridad de control en materia de protección de datos, una instancia colegiada o una autoridad unipersonal son perfectamente competentes para ejercer su función, lo relevante es su independencia y las atribuciones, poderes y recursos con los que cuenten para tutelar la protección de datos de carácter personal, por lo que en definitiva su diseño institucional dependerá de la tradición administrativa, la eficacia y eficiencia que uno u otro sistema, colegiado o unipersonal, haya demostrado en el respectivo Estado donde se pretenda instalar.

A nivel europeo existen varias estructuras o sistemas de protección de los derechos humanos que contribuyen a garantizar la protección efectiva de los derechos fundamentales en la UE, en particular aquellos protegidos por la CDFUE. Estos mecanismos alternativos y especializados de protección son instrumentos esenciales en la tarea de garantizar los derechos fundamentales… tales como la Agencia de los Derechos Fundamentales de la Unión Europea (FRA) y el Supervisor Europeo de Protección de Datos (SEPD), en la evolución de la legislación europea del derecho fundamental a la protección de datos[482].

4. Rendición de cuentas y transparencia

Este principio destaca la relevancia de la rendición de cuentas y la transparencia para los reguladores económicos. De hecho, la rendición de cuentas y la transparencia son las bases de la confianza, pero también un mecanismo para alinear las expectativas entre los reguladores y

[482] Martínez López-Sáez, M., (2018), "Una revisión del derecho fundamental a la protección de datos de carácter personal", Tirant Lo Blanch, Valencia, p. 126.

los actores involucrados. El mensaje central del principio es que las prácticas obligatorias o auto impuestas en la rendición de cuentas y transparencia promueven el proceso de toma de decisiones y brindan elementos para reducir el riesgo de captura regulatoria.

Usualmente, los gobiernos mantienen las obligaciones de transparencia y rendición de cuentas para todos los entes públicos, incluidos los reguladores. No obstante, los reguladores independientes deben ir más allá de estos deberes en comparación con todos los entes públicos; por ello, mientras los reguladores avancen hacia la independencia o la autonomía, deben aumentar sus prácticas de rendición de cuentas y transparencia para fortalecer la confianza.

Las obligaciones de rendir cuentas podrían incluir al Ejecutivo, el Congreso, al público y los diferentes actores interesados. Por supuesto, los conceptos para la rendición de cuentas no son necesariamente los mismos para todos los actores. El Ejecutivo, por ejemplo, podría enfocarse en los objetivos de política, la coordinación con los ministerios y la ejecución del presupuesto; el Congreso podría enfocarse en los objetivos de política y la ejecución presupuestal; y el público y los actores involucrados podrían hacerlo en los objetivos de política. En estos temas, es relevante que los reguladores publiquen sus planes operativos para cada año, de modo que los actores interesados puedan comparar la agenda planeada con los resultados alcanzados.

En perspectiva, la transparencia es una especie de rendición de cuentas para el público, y los beneficios de publicar la información vale el trabajo adicional que ello implica. Por tanto, los reguladores deben publicar toda la información posible acerca de su operación; por ejemplo, la ejecución presupuestal, las estadísticas de la industria, planes anuales de trabajo, reuniones con actores involucrados y sus minutas, metas y objetivos alcanzados. Esta información debe ser de fácil localización para la mayoría de los usuarios potenciales y en formatos manejables. También se recomienda que los reguladores pongan atención en los datos que necesitan los usuarios y los incluyan en las estadísticas diarias. En pocas palabras, los reguladores deben seguir una política de transparencia como mecanismo para obtener la confianza.

Sobre este principio, el RGPD consagra el deber de la autoridad de control de elaborar un informe anual de sus actividades. Así se establece en el artículo 59, que señala que “Cada autoridad de control elaborará un informe anual de sus actividades, que podrá incluir una lista de tipos de infracciones notificadas y de tipos de medidas adoptadas de conformidad con el artículo 58, apartado 2. Los informes se transmitirán al Parlamento nacional, al Gobierno y a las demás autoridades designadas en virtud del Derecho de los Estados miembros. Se pondrán a disposición del público, de la Comisión y del Comité”.

La AEPD ha elaborado una memoria anual de las actividades desarrolladas por el organismo desde 1994, año en el que comenzó su actividad. Estas memorias han sido publicadas y se encuentran disponibles en la página web de la Agencia.

Por otra parte, desde el año 2004 también publica el organismo todas las resoluciones dictadas por el Director como consecuencia de los procedimientos tramitados en relación con las denuncias y solicitudes de tutela de derechos presentadas ante la Agencia, y sobre el resto de procedimientos que tramita, como autorizaciones de transferencias internacionales y códigos tipo.

La página web de la Agencia y su sede electrónica ofrecen una importante cantidad de información que incluye guías, recomendaciones, herramientas de ayuda, documentación sobre las jornadas y actividades que convoca, así como toda la información correspondiente a

la publicidad activa de la Agencia que se encuentra en el apartado de transparencia de la Agencia[483].

5. Participación y compromiso de los actores interesados

Este principio se refiere al compromiso de la agencia regulatoria de interactuar con los entes regulados y otros actores involucrados. La relevancia de generar un compromiso con los actores involucrados se debe a que los reguladores aprenden de la industria la forma en que esta funciona.

El compromiso con los actores involucrados es también un mecanismo para producir regulación de calidad ya que puede brindar retroalimentación acerca de un problema específico y propuestas para resolverlo. A través de la participación con los actores interesados los reguladores pueden presentar opiniones sobre problemas potenciales, acerca de los efectos de la regulación, pero también pueden anticipar la regulación y reducir los costos de implementación y la incertidumbre.

Es importante que los reguladores se comprometan con una política de participación de los actores interesados. La mayoría de los reguladores tienen contacto activo con las empresas que regulan y otros actores, pero esta es una práctica diferente desde un enfoque de políticas. Una política de participación de los actores involucrados requiere, por ejemplo, objetivos, una agenda programada y planeada para discutir asuntos regulatorios, además de un análisis de los temas de discusión.

Las iniciativas de involucramiento y participación de actores interesados se recomiendan ampliamente, pero los reguladores deben tomar en consideración las mejores prácticas en dichas actividades, para evitar riesgos de captura regulatoria y conflicto de intereses. Al mismo tiempo, los reguladores deben ser claros con el objetivo de estas actividades, de modo que los actores involucrados ajusten sus expectativas.

Finalmente, según la OCDE todos los ejercicios deben adecuarse al propósito, esto significa que las expectativas requieren un criterio de racionalidad. Por ejemplo, podría ser excesivo realizar una consulta compleja, costosa e integral *in situ* para una regulación propuesta de bajo alcance y con pocos efectos potenciales previstos. Por ello, es importante adoptar prácticas de consulta como la consulta temprana y la consulta ex post (al amparo de las actividades de evaluación ex post) como parte de la política de compromiso.

Por lo expuesto parece interesante la experiencia de algunos modelos de autoridades de control en materia de protección de datos que han incluido en sus estructuras organizacionales consejos de la sociedad civil o de la industria o sectores regulados, lo que les permite tener una interacción y mayor retroalimentación, debiendo eso sí, tal como se ha indicado, evitar capturas regulatorias o eventuales conflictos de interés.

La literatura sobre la participación de la sociedad civil, se puede analizar desde diferentes aspectos, iniciando por el hecho de que existen varias definiciones de sociedad civil, para

[483] Blanco Antón, M., (2019), "Autoridades de Control Independientes (Arts. 51-59 RGPD). Autoridades de Protección de Datos (Arts. 44-59 y Disposición adicional cuarta LOPDGDD)", pp. 634-635, en "*La Adaptación al Nuevo Marco de Protección de Datos tras el RGPD y la LOPDGDD"*, Coordinador José López Calvo, Boch Wolters Kluwer.

nuestro propósito es suficiente decir que cubre todas las actividades que son independientes de los Estados y mercados, basadas en una actividad voluntaria sin ánimo de lucro. La sociedad civil está integrada por organizaciones no gubernamentales, organizaciones sin ánimo de lucro, comunitarias, de autoayuda, sindicatos, religiosas y cooperativas, voluntariado, movilización social, acción colectiva y demás manifestaciones de la sociedad civil[484].

Por otra parte, la industria o los sectores regulados tratan cantidades impresionantes de información, que son creadas y contenidas en conjuntos de datos de una magnitud tan alta que los métodos tradicionales de análisis no son adecuados para manejarlos. Esto es lo que se ha denominado «*big data*», un conjunto de información tan voluminoso y complejo que escapa al concepto de procesamiento de datos tradicional. Actualmente, todas las empresas más importantes de internet, como Facebook, Google, Ebay, Microsoft y Amazon, entre otras, participan en *big data*. La idea detrás es simple: los datos son información y ello proporciona una ventaja competitiva que se transforma en ingresos. Entre más datos, más ganancias. Una parte importante de esta información se refiere a las preferencias, los hábitos, las características y el comportamiento de personas identificadas o identificables. Así, a través del análisis computarizado de datos, las compañías generan perfiles de usuarios que actualmente se extienden a cada aspecto y fase de la vida individual y social de las personas. Esta información tiene una gran importancia económica, ya que se utiliza para crear valor agregado e innovación en la economía digital actual[485].

6. Financiamiento

El principio tiene al menos dos vertientes. En primer lugar, el financiamiento es el canal que permite al regulador alcanzar las metas de acuerdo con los objetivos. Por otro lado, las fuentes de financiamiento pueden contribuir a asegurar la independencia (principalmente del gobierno, pero también de las empresas reguladas) en el proceso de toma de decisiones y la implementación de la regulación.

La cantidad de recursos disponibles para los reguladores debe ser planeada conforme a los objetivos y de acuerdo con las metas que se busca alcanzar. El financiamiento para los reguladores debe ser justamente lo suficiente para lograr las metas esperadas de acuerdo con el cronograma previsto, que puede incluir objetivos anuales o a un plazo mayor. De hecho, la planeación de las metas y el presupuesto están alineados de forma muy cercana. Aun así, el presupuesto no debe ser el principal impulsor, ya que en ocasiones un presupuesto más ajustado se asigna para alcanzar metas altas. No significa, por el contrario, que el regulador debe tener grandes presupuestos, más que eso, el presupuesto y las metas deben estar en equilibrio y la clave es la planeación.

Las fuentes de financiamiento y disponibilidad real en el tiempo son también un tema relevante para fines de independencia. La independencia se apoya en los arreglos institucionales entre

---

[484] Morales Tostado, María del Carmen, Monterde Valenzuela, María de los Ángeles, & Morales Tostado, Reyna Guadalupe. (2020). Participación de la sociedad civil en el derecho de acceso a la información pública. *Biolex*, *12*(22), 79-103. Epub 28 de abril de 2021.https://doi.org/10.36796/biolex.v22i0.164

[485] Frigerio Dattwyler, Catalina. (2018). Mecanismos de regulación de datos personales: una mirada desde el análisis económico del derecho. *Revista chilena de derecho y tecnología*, *7*(2), 45-80. https://dx.doi.org/10.5354/0719-2584.2018.50578

reguladores y entes responsables de brindar el financiamiento. Estos arreglos podrían ser sólidos y podrían no ser necesarios para separar el presupuesto del regulador de otras instituciones, como ocurre cuando el organismo es parte de un ministerio o aquél valida el presupuesto.

Si los arreglos son fuertes al paso del tiempo, es posible mantener dicha estructura, pero si existe una percepción de un riesgo que cambie la política, es sensible separar el presupuesto del ministerio a través de instrumentos jurídicos. Asignarle facultades jurídicas al regulador para evaluar, proponer, presentar e implementar el presupuesto ayuda a reducir el riesgo de captura y mitiga posibles presiones que puedan influenciar las decisiones de los reguladores. Los arreglos particulares acerca del presupuesto dependen de los perfiles de cada país y de la capacidad institucional, pero vale la pena mencionar que la planeación y ejecución de un presupuesto propio van encaminadas rumbo a la independencia.

El Informe de Evaluación de aplicación del RGPD de la Comisión Europea del 24 de junio de 2020, se refiere al financiamiento y los recursos humanos y presupuestarios de las autoridades de control de protección de datos personales, al señalar: "…deben recibir el apoyo adecuado en forma de recursos humanos, técnicos y financieros. Muchos Estados miembros lo están haciéndolo así y han incrementado notablemente las dotaciones presupuestarias y de personal. En general, se ha registrado un aumento del 42% en el personal y del 49 % en el presupuesto en el conjunto de las autoridades nacionales de protección de datos de la UE entre 2016 y 2019. Sin embargo, existen todavía diferencias radicales entre los Estados miembros".

7. Evaluación del desempeño

Este principio incentiva que los reguladores lleven a cabo una evaluación del desempeño de acuerdo con los objetivos planteados. Si el regulador no evalúa su trabajo y acciones, nunca sabrá si los efectos de su intervención están alineados con sus objetivos y si los recursos invertidos tienen utilidades.

La evaluación del desempeño permite a los reguladores fortalecer las actividades o acciones que contribuyen a la mayoría de sus metas y modifican aquellas con efectos deficientes. Debido a la relevancia de la evaluación del desempeño, es importante realizar estos ejercicios de forma periódica. La frecuencia depende de la importancia de la política y el tipo de evaluación. Por ejemplo, una evaluación de indicadores del desempeño sobre los resultados puede ser anual, ya que requiere un análisis estadístico "simple" con bajo consumo de tiempo. Por otro lado, el impacto o efectos reales de las decisiones regulatorias requieren un análisis que son herramientas más complejas y avanzadas. Al mismo tiempo, la identificación de los efectos finales puede no ser tan clara en las primeras etapas de implementación.

Finalmente, tan importante como la presentación de las actividades de evaluación del desempeño es la publicación de los resultados el que se añade a los temas de rendición de cuentas y transparencia[486].

[486] Sobre la evaluación y publicidad de resultados el RGPD prevé que la Comisión Europea informe sobre la aplicación y la revisión de dicho Reglamento, empezando por un primer informe al cabo de los dos primeros años de aplicación y cada cuatro años a partir de entonces. El primer informe se dio a conocer el 24 de junio de 2020, el cual es posible consultar en: https://ec.europa.eu/info/files/gdpr-report-communication-swd_en

La Autoridad de Control en la Directiva 95/46 del Consejo de Europa

La Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, regulaba la autoridad de control en su artículo 28 al señalar[487]:

"Autoridad de control

Los Estados miembros dispondrán que una o más autoridades públicas se encarguen de vigilar la aplicación en su territorio de las disposiciones adoptadas por ellos en aplicación de la presente Directiva.

Estas autoridades ejercerán las funciones que les son atribuidas con total independencia.

Los Estados miembros dispondrán que se consulte a las autoridades de control en el momento de la elaboración de las medidas reglamentarias o administrativas relativas a la protección de los derechos y libertades de las personas en lo que se refiere al tratamiento de datos de carácter personal.

La autoridad de control dispondrá, en particular, de:

- *poderes de investigación, como el derecho de acceder a los datos que sean objeto de un tratamiento y el de recabar toda la información necesaria para el cumplimiento de su misión de control;*
- *poderes efectivos de intervención, como, por ejemplo, el de formular dictámenes antes de realizar los tratamientos, con arreglo al artículo 20, y garantizar una publicación adecuada de dichos dictámenes, o el de ordenar el bloqueo, la supresión o la destrucción de datos, o incluso prohibir provisional o definitivamente un tratamiento, o el de dirigir una advertencia o amonestación al responsable del tratamiento o el de someter la cuestión a los parlamentos u otras instituciones políticas nacionales;*
- *capacidad procesal en caso de infracciones a las disposiciones nacionales adoptadas en aplicación de la presente Directiva o de poner dichas infracciones en conocimiento de la autoridad judicial.*

Las decisiones de la autoridad de control lesivas de derechos podrán ser objeto de recurso jurisdiccional.

Toda autoridad de control entenderá de las solicitudes que cualquier persona, o cualquier asociación que la represente, le presente en relación con la protección de sus derechos y libertades respecto del tratamiento de datos personales. Esa persona será informada del curso dado a su solicitud.

Toda autoridad de control entenderá, en particular, de las solicitudes de verificación de la licitud de un tratamiento que le presente cualquier persona cuando sean de aplicación las disposiciones nacionales tomadas en virtud del artículo 13 de la

[487] Y también se refería a la importancia de crear un Autoridad de control en cada Estado miembro para la adecuada tutela del tratamiento de datos personales. Así disponía el considerando 62 de dicha Directiva: "Considerando que la creación de una autoridad de control que ejerza sus funciones con plena independencia en cada uno de los Estados miembros constituye un elemento esencial de la protección de las personas en lo que respecta al tratamiento de datos personales".

presente Directiva. Dicha persona será informada en todos los casos de que ha tenido lugar una verificación.
Toda autoridad de control presentará periódicamente un informe sobre sus actividades. Dicho informe será publicado.
Toda autoridad de control será competente, sean cuales sean las disposiciones de Derecho nacional aplicables al tratamiento de que se trate, para ejercer en el territorio de su propio Estado miembro los poderes que se le atribuyen en virtud del apartado 3 del presente artículo. Dicha autoridad podrá ser instada a ejercer sus poderes por una autoridad de otro Estado miembro.
Las autoridades de control cooperarán entre sí en la medida necesaria para el cumplimiento de sus funciones, en particular mediante el intercambio de información que estimen útil.
Los Estados miembros dispondrán que los miembros y agentes de las autoridades de control estarán sujetos, incluso después de haber cesado en sus funciones, al deber de secreto profesional sobre informaciones confidenciales a las que hayan tenido acceso".

Como se puede observar, ya la señalada Directiva establecía la existencia de entidades públicas que asumieran institucionalmente en cada Estado miembro de la Unión, la protección de datos de carácter personal. Agencias independientes dotadas de poderes o facultades de investigación, intervención y habilitadas, si es necesario, para comparecer en juicio. Constituyéndose en un sistema de garantías del derecho fundamental a la protección de datos en la Unión Europea, ampliamente analizado por la doctrina[488].

Un aspecto interesante es el poder que la Directiva le asigna a la Autoridad de Control para emitir dictámenes, de conformidad a lo señalado en el artículo 20[489] de la misma, por cuanto implica que esta entidad tiene capacidad normativa o potestad dictaminante, lo que significa que está facultada para dictar actos administrativos de tipo normativo, que son vinculantes para sus destinatarios, generando jurisprudencia administrativa en la tutela de la protección de datos de carácter personal, ordenando la supresión de datos, su bloqueo, autorizando o prohibiendo el tratamiento de los mismos, advirtiendo o sancionando al responsable de su tratamiento e incluso ordenando destruir los datos.

Además, la Directiva reconoce que las actuaciones de la Autoridad de control son susceptibles de ser impugnadas por la vía jurisdiccional, lo que sigue la regla general de los ordenamientos jurídicos en orden a que los actos administrativos son impugnables ante los tribunales de justicia.

---

[488] Ramiro Arenas, M. (2006), "El derecho fundamental a la protección de datos personales en Europa". Tirant lo Blanch, Vlencia, pp. 363-374.

[489] "Controles previos 1. Los Estados miembros precisarán los tratamientos que puedan suponer riesgos específicos para los derechos y libertades de los interesados y velarán por que sean examinados antes del comienzo del tratamiento. 2. Estas comprobaciones previas serán realizadas por la autoridad de control una vez que haya recibido la notificación del responsable del tratamiento o por el encargado de la protección de datos quien, en caso de duda, deberá consultar a la autoridad de control. 3. Los Estados miembros podrán también llevar a cabo dicha comprobación en el marco de la elaboración de una norma aprobada por el Parlamento o basada en la misma norma, que defina el carácter del tratamiento y establezca las oportunas garantías".

También el apartado 4 del artículo 28 de la Directiva, establece el deber de información que tiene la Autoridad de Control, en orden a mantener al tanto del curso de una solicitud que cualquier persona o asociación le presente, relativa al tratamiento de datos de carácter personal que le afecte, así como informar respecto de la licitud del tratamiento según lo dispone el artículo 13 de la Directiva 95/46/CE[490]. Este deber de información se refuerza también con el acceso a la información y deber de transparencia que la Autoridad de Control debe realizar presentando periódicamente un informe sobre sus actividades y gestiones, el que será público.

El artículo 28 en análisis, reconoce también la competencia que tiene la autoridad de control para actuar y ejercer sus poderes en el territorio del respectivo Estado donde esta se encuentre, lo que también sigue la regla de la territorialidad en materia competencial, en el sentido de que el territorio es uno de los elementos que conforman la competencia y que habilitan al órgano público, en este caso a la Autoridad de Control, para actuar en el ámbito espacial o territorio de su respectivo Estado, ya que así lo ha habilitado, es decir, autorizado y facultado, la Directiva 95/46/CE.

El apartado 6 del artículo 28 reconoce también la cooperación que debe existir entre las distintas autoridades de control de los Estados miembros, generando las sinergias y colaboraciones necesarias para el adecuado resguardo en el tratamiento de datos de las personas físicas, como se verá más adelante en este trabajo, el RGPD profundiza mucho más en el principio de cooperación entre las agencias de control.

Finalmente, el apartado 7 y final del artículo 28 de la Directiva, impone a los integrantes de las autoridades de control el deber de secreto profesional sobre la información confidencial a la que hayan tenido acceso en el ejercicio de su función pública, sin disponer un lapso o plazo específico para ello, lo que resulta del todo coherente para la efectiva tutela de los datos personales a los que hayan tenido acceso.

El artículo 29 de la Directiva 95/46/CE[491] estableció la existencia de un Grupo de Trabajo sobre Protección de Datos, que elaboró entre otros el documento "Directrices para determinar

[490] "Excepciones y limitaciones 1. Los Estados miembros podrán adoptar medidas legales para limitar el alcance de las obligaciones y los derechos previstos en el apartado 1 del artículo 6, en el artículo 10, en el apartado 1 del artículo 11, y en los artículos 12 y 21 cuando tal limitación constituya una medida necesaria para la salvaguardia de: a) la seguridad del Estado; b) la defensa; c) la seguridad pública) la prevención, la investigación, la detección y la represión de infracciones penales o de las infracciones de la deontología en las profesiones reglamentadas; e) un interés económico y financiero importante de un Estado miembro o de la Unión Europea, incluidos los asuntos monetarios, presupuestarios y fiscales; f) una función de control, de inspección o reglamentaria relacionada, aunque sólo sea ocasionalmente, con el ejercicio de la autoridad pública en los casos a que hacen referencia las letras c), d) y e); g) la protección del interesado o de los derechos y libertades de otras personas. 2. Sin perjuicio de las garantías legales apropiadas, que excluyen, en particular, que los datos puedan ser utilizados en relación con medidas o decisiones relativas a personas concretas, los Estados miembros podrán, en los casos en que manifiestamente no exista ningún riesgo de atentado contra la intimidad del interesado, limitar mediante una disposición legal los derechos contemplados en el artículo 12 cuando los datos se vayan a tratar exclusivamente con fines de investigación científica o se guarden en forma de archivos de carácter personal durante un período que no supere el tiempo necesario para la exclusiva finalidad de la elaboración de estadísticas".

[491] "Grupo de protección de las personas en lo que respecta al tratamiento de datos personales. 1. Se crea un grupo de protección de las personas en lo que respecta al tratamiento de datos personales, en lo sucesivo denominado "Grupo". Dicho Grupo tendrá carácter consultivo e independiente. 2. El Grupo estará compuesto por un representante de la autoridad o de las autoridades de control designadas por cada Estado miembro, por un representante de la autoridad o autoridades creadas por las instituciones y organismos comunitarios, y por un

la autoridad de control principal de un responsable o encargado del tratamiento", las que se establecieron inicialmente el 13 de diciembre de 2016, revisadas por última vez y adoptadas el 5 de abril de 2017.

El Grupo de Trabajo es un órgano consultivo independiente de la UE en materia de protección de datos y privacidad. Sus funciones se describen en el artículo 30 de la Directiva 95/46/CE, el cual señala:

> "*1. El Grupo tendrá por cometido: a) estudiar toda cuestión relativa a la aplicación de las disposiciones nacionales tomadas para la aplicación de la presente Directiva con vistas a contribuir a su aplicación homogénea; b) emitir un dictamen destinado a la Comisión sobre el nivel de protección existente dentro de la Comunidad y en los países terceros; c) asesorar a la Comisión sobre cualquier proyecto de modificación de la presente Directiva, cualquier proyecto de medidas adicionales o específicas que deban adoptarse para salvaguardar los derechos y libertades de las personas físicas en lo que respecta al tratamiento de datos personales, así como sobre cualquier otro proyecto de medidas comunitarias que afecte a dichos derechos y libertades; d) emitir un dictamen sobre los códigos de conducta elaborados a escala comunitaria. 2. Si el Grupo comprobare la existencia de divergencias entre la legislación y la práctica de los Estados miembros que pudieren afectar a la equivalencia de la protección de las personas en lo que se refiere al tratamiento de datos personales en la Comunidad, informará de ello a la Comisión. 3. El Grupo podrá, por iniciativa propia, formular recomendaciones sobre cualquier asunto relacionado con la protección de las personas en lo que respecta al tratamiento de datos personales en la Comunidad. 4. Los dictámenes y recomendaciones del Grupo se transmitirán a la Comisión y al Comité contemplado en el artículo 31. 5. La Comisión informará al Grupo del curso que haya dado a los dictámenes y recomendaciones. A tal efecto, elaborará un informe, que será transmitido asimismo al Parlamento Europeo y al Consejo. Dicho informe será publicado. 6. El Grupo elaborará un informe anual sobre la situación de la protección de las personas físicas en lo que respecta al tratamiento de datos personales en la Comunidad y en los países terceros, y lo transmitirá al Parlamento Europeo, al Consejo y a la Comisión. Dicho informe será publicado".*

Las directrices disponen sobre la determinación de la autoridad de control principal que, "una autoridad de control principal es la autoridad que asume la responsabilidad principal sobre una actividad de tratamiento transfronterizo, por ejemplo, cuando un interesado presenta una queja sobre el tratamiento de sus datos personales. La autoridad de control principal coordinará cualquier investigación, haciendo partícipes a otras autoridades de control "interesadas". La determinación de la autoridad de control principal depende de la determinación de la ubicación

representante de la Comisión. Cada miembro del Grupo será designado por la institución, autoridad o autoridades a que represente. Cuando un Estado miembro haya designado varias autoridades de control, éstas nombrarán a un representante común. Lo mismo harán las autoridades creadas por las instituciones y organismos comunitarios. 3. El Grupo tomará sus decisiones por mayoría simple de los representantes de las autoridades de control. 4. El Grupo elegirá a su presidente. El mandato del presidente tendrá una duración de dos años. El mandato será renovable. 5. La Comisión desempeñará las funciones de secretaría del Grupo. 6. El Grupo aprobará su reglamento interno. 7. El Grupo examinará los asuntos incluidos en el orden del día por su presidente, bien por iniciativa de éste, bien previa solicitud de un representante de las autoridades de control, bien a solicitud de la Comisión".

del "establecimiento principal" o del "establecimiento único" del responsable del tratamiento en la UE".

La Autoridad de Control en el Reglamento General de Protección de Datos RGPD 679/2016

Más allá de las directrices establecidas por el Grupo de trabajo, a diferencia de la Directiva 95/46/CE, que como se analizó hacía referencia a la Autoridad de Control -sus características, poderes y funciones- únicamente en el artículo 28, el RGPD tiene varios artículos, del 51 al 59, insertos en el capítulo VI cuyo título precisamente es "Autoridades de control independientes", donde se aborda respecto de estas entidades su independencia (artículo 52), condiciones generales aplicables a sus miembros (artículo 53), normas relativas a su establecimiento (artículo 54), competencia (artículo 55), competencia de la autoridad de control principal (artículo 56), funciones (artículo 57), poderes (artículo 58) e informe de sus actividades (artículo 59). Disposiciones que se pueden complementar con los artículos 60, 61, 62 y 63 relacionados con la cooperación, asistencia mutua y coherencia que debe existir entre las distintas autoridades de control. A mayor abundamiento, entre los considerandos 117 a 138 el Reglamento se refiere también al establecimiento, características, poderes, funciones y otras materias relacionadas con la Autoridad de control[492].

El capítulo VI del RGPD fortalece las facultades e independencia de las autoridades de control para la protección de datos de carácter personal, estableciendo mayores sanciones económicas en caso de incumplimiento e incentivando la colaboración y coherencia de la normativa de protección de datos en todos los Estados de la Unión Europea.

El Reglamento, tanto en su artículo 51 como en su considerando 117, se refieren al establecimiento de las autoridades de control, reconociendo la posibilidad de que en cada Estado miembro pueda existir más de una, dependiendo de su estructura constitucional, organizativa y administrativa.

Esto significa también el reconocimiento de que cada Estado puede establecer entidades sub-nacionales encargadas de la protección de datos, como por ejemplo ocurre en España con las Comunidades Autónomas, en los casos de la Autoridad Catalana, Vasca y de Andalucía en materia de protección de datos de carácter personal en el ámbito del sector público catalán, vasco y andaluz, respectivamente, lo que dependerá de la forma en que se estructure la administración del respectivo país, sea de manera más centralizada o de manera más descentralizada. En este caso, es decir cuando exista más de una Autoridad de control, el respectivo Estado miembro designará a la autoridad nacional que lo representará ante el Comité Europeo de Protección de Datos que en el caso español es la Agencia Española de Protección de Datos.

[492] El RGPD que incluye un total de 173 considerandos y 99 artículos es obligatorio para cada Estado miembro, y tiene un contenido extenso y detallado en cada una de las materias que aborda, así también ocurre con lo relativo a la Autoridad de Control..

Además del establecimiento de la Autoridad de control y como señala el considerando 117[493] del RGPD, un "elemento esencial" es también la independencia que dicha autoridad tenga. De eso ya daban cuenta tanto la Carta de Derechos Fundamentales de la Unión Europea CDFUE y el Tratado de Funcionamiento de la Unión Europea TFUE. En efecto, la CDFUE establece en su artículo 8.3, a propósito del derecho a la protección de datos de carácter personal que "El respeto de estas normas estará sujeto al control de una autoridad independiente". Y el TFUE en su artículo 16.2 dispone:

> *"El Parlamento Europeo y el Consejo establecerán, con arreglo al procedimiento legislativo ordinario, las normas sobre protección de las personas físicas respecto del tratamiento de datos de carácter personal por las instituciones, órganos y organismos de la Unión, así como por los Estados miembros en el ejercicio de las actividades comprendidas en el ámbito de aplicación del Derecho de la Unión, y sobre la libre circulación de estos datos. El respeto de dichas normas estará sometido al control de autoridades independientes".*

Ya el Tribunal de Justicia de la Unión Europea TJUE, en el año 2015 a propósito del caso Schrems, o también conocido como Acuerdo de puerto Puerto Seguro [494], se refería a la

---

[493] "El establecimiento en los Estados miembros de autoridades de control capacitadas para desempeñar sus funciones y ejercer sus competencias con plena independencia constituye un elemento esencial de la protección de las personas físicas con respecto al tratamiento de datos de carácter personal. Los Estados miembros deben tener la posibilidad de establecer más de una autoridad de control, a fin de reflejar su estructura constitucional, organizativa y administrativa".

[494] Los hechos del caso dicen relación con una reclamación presentada ante la autoridad irlandesa de protección de datos personales -el Comisario Irlandés de Protección de Datos *(Data Protection Commissioner)*- por parte de Maximilian Schrems, un joven jurista austriaco residente en Irlanda. Tal como se menciona brevemente en la sentencia, el caso tiene directa relación con las filtraciones de Edward Snowden a propósito de algunos programas de vigilancia masiva implementados por la Agencia Nacional de Seguridad de Estados Unidos (*National Security Agency* o NSA) y otras agencias colaboradoras, como el Cuartel General de Comunicaciones del Gobierno del Reino Unido (*Government Communications Headquarters* o GCHQ). Con posterioridad a los atentados del 11 de septiembre de 2001, y con la supuesta finalidad de prevenir ataques terroristas, la implementación de estos programas permitió recolectar de manera masiva los datos personales de millones de usuarios de los servicios de telecomunicación a lo largo y ancho del globo.

La tecnología utilizada para tal efecto razonaba sobre la lógica del *Big Data,* con lo cual los datos no eran recopilados selectivamente, sino a gran escala, incluyendo la información de personas no sospechosas de cometer o planificar un delito. Los datos recopilados eran procesados con el supuesto objetivo de recabar información útil para la prevención y sanción de delitos terroristas. El alcance de estas operaciones era transfronterizo, afectando no solo a ciudadanos norteamericanos, sino también a todo el mundo. Para coronar lo anterior, los programas eran puestos en marcha con absoluto secreto y casi sin garantías de revisión judicial, contando además con un sustento jurídico formal en la normativa interna.

Pues bien, el joven Schrems era usuario de Facebook, una de las empresas de telecomunicación más importantes del mundo. Facebook tiene una importante filial en Irlanda, Facebook Ireland, que se encarga de transferir a Estados Unidos los datos personales de todos los usuarios europeos.

En su reclamación ante el Comisario Irlandés de Protección de Datos, Schrems alegaba que las revelaciones de Snowden demostraban que Estados Unidos no aseguraba un nivel adecuado de protección respecto de los datos personales que se transferían a ese país. Con base en lo anterior, Schrems solicitó que se prohibiera la transferencia de datos a Estados Unidos. El Comisario Irlandés rechazó la solicitud, argumentando que la Decisión de la Comisión presumía que Estados Unidos cumplía con un nivel de protección adecuado. Además, indicó que no tenía el deber de investigar los hechos, dado que el demandante no había aportado pruebas suficientes para demostrar que la NSA había accedido efectivamente a sus datos personales.

importancia de las autoridades de control y su independencia, para la adecuada tutela de la protección de datos de carácter personal, al señalar en su considerando 41: "La garantía de independencia de las autoridades nacionales de control pretende asegurar un control eficaz y fiable del respeto de la normativa en materia de protección de las personas físicas frente al tratamiento de datos personales y debe interpretarse a la luz de dicho objetivo. Esa garantía se ha establecido para reforzar la protección de las personas y de los organismos afectados por las decisiones de dichas autoridades. La creación en los Estados miembros de autoridades de control independientes constituye, pues, un elemento esencial de la protección de las personas frente al tratamiento de datos personales".

Hay además, según Troncoso Reigada[495], tres sentencias del TJUE anteriores al RGPD y, por lo tanto, dictadas bajo la vigencia de la Directiva 95/46/CE, que analizan la independencia de las autoridades de control, "…la STJUE, de 8 de abril de 2014 - Asunto C-288712 Comisión/Hungría -, en relación con la inamovilidad de sus miembros, donde el Tribunal declaró que Hungría habría incumplido las obligaciones de la Directiva "al poner fin antes de tiempo al mandato de la autoridad de control de la protección de datos personales". También señala, está la STJUE, de 16 de octubre de 2012- Asunto C-614/10 Comisión/Austria -, en relación con la autonomía organizativa y de personal y a la independencia funcional de la autoridad de control, donde el Tribunal declaró que Austria había incumplido las obligaciones de la Directiva "al no haber adoptado las medidas necesarias para que la legislación vigente en Austria cumpla el requisito de la independencia en lo que se refiere a la Comisión de protección de datos", al mantener un marco normativo en virtud del cual el administrador de la Comisión es un funcionario federal sometido a supervisión jerárquica, la secretaría de la Comisión está integrada por la Cancillería federal y el Canciller federal tiene un derecho incondicional a informarse de todos los aspectos de la gestión de la Comisión".

Finalmente, agrega una tercera STJUE de 9 de marzo de 2010 – Asunto C-518/07 Comisión/Alemania –, también en relación con la autonomía organizativa y donde el Tribunal declaró que la República Federal de Alemania había incumplido las obligaciones de la Directiva "al someter a la tutela del Estado a las autoridades de control encargadas de vigilar en los diferentes *Länders* el tratamiento de datos personales efectuado por los organismos no

---

Tras esta primera derrota, Schrems presentó un recurso ante la Alta Corte de Irlanda. A diferencia del pronunciamiento anterior, este tribunal consideró que las revelaciones de Snowden habían demostrado injerencias excesivas de Estados Unidos en el tratamiento de los datos personales. Además, estimó que la interpretación de la Decisión de la Comisión Europea a la luz de la Directiva 95/46/CE planteaba un problema de implementación del derecho de la Unión Europea por parte de los Estados miembros con base en el artículo 51 CDFUE, con lo cual decidió elevar una cuestión prejudicial al TJUE. Mediante dicho mecanismo la Alta Corte planteó lo siguiente:

1) En primer lugar, consultó si el Comisario Irlandés estaba vinculado por la protección de los derechos fundamentales consagrados en la Carta de Niza, a pesar de que la decisión presumía que Estados Unidos garantizaba un nivel adecuado de protección.

2) En segundo lugar, planteó si el Comisario Irlandés podía iniciar una investigación independiente, sin perjuicio de lo dispuesto en esta decisión.

El 23 de septiembre de 2015, el Abogado General Yves Bot emitió sus conclusiones y el 6 de octubre del mismo año, actuando como Gran Sala, el TJUE dictó la sentencia objeto de análisis.

[495]Troncoso Reigada, A. (2016), "Autoridades de Control Independientes", en *Reglamento General de Protección de Datos, Hacia un nuevo modelo europeo de privacidad*, director, José Luis Piñar Mañas, Reus, Madrid, p. 473.

públicos y las empresas públicas que compitan en el mercado y al haber adaptado así incorrectamente su normativa nacional a la exigencia de que dichas autoridades ejerzan sus funciones con total independencia".

Elementos de la independencia de los miembros y de la propia Autoridad de Control en el RGPD

La autonomía[496] o independencia, entonces, es un elemento consustancial a la Autoridad de control, cuyo establecimiento constituye una garantía esencial para el resguardo de la protección de datos de carácter personal, lo que se expresa en la ausencia de toda tutela o dependencia alguna para el desempeño de sus funciones[497]. El RGPD estructura esta independencia sobre la base de elementos que inciden en los miembros o integrantes de la Autoridad de control como en el funcionamiento mismo de dicha Autoridad.

En efecto, respecto de los elementos que configuran la independencia de los miembros o integrantes de la Autoridad de control, es posible distinguir la forma en que son designados y los requisitos para ello, además del tiempo en que ejercerán sus funciones, así como la inamovilidad de la que gozan y las incompatibilidades que los afectan.

Con relación a los elementos que estructuran la independencia del funcionamiento de la Autoridad de control, se distinguen fundamentalmente la autonomía de personal, presupuestaria y financiera, de la que gozan para el desempeño de sus funciones.

Ilustrativo sobre los elementos que configuran la independencia de la Autoridad de control es el considerando 121 del RGPD, que señala:

> *"Las condiciones generales aplicables al miembro o los miembros de la autoridad de control deben establecerse por ley en cada Estado miembro y disponer, en particular, que dichos miembros han de ser nombrados, por un procedimiento transparente, por el Parlamento, el Gobierno o el jefe de Estado del Estado miembro, a propuesta del Gobierno, de un miembro del Gobierno o del Parlamento o una de sus cámaras, o por un organismo independiente encargado del nombramiento en virtud del Derecho de los Estados miembros. A fin de garantizar la independencia de la autoridad de control, sus miembros deben actuar con integridad, abstenerse de cualquier acción que sea incompatible con sus funciones y no participar, mientras dure su mandato, en ninguna actividad profesional incompatible, sea o no remunerada. La autoridad de control*

[496] En el ordenamiento jurídico chileno se hace referencia a la autonomía y no a la independencia para hacer referencia a los órganos de la administración del Estado que son independientes del Presidente de la República. La autonomía es un concepto jurídico indeterminado, ya que ni la Constitución chilena ni la ley la definen, no obstante, reconocen la existencia de organismos autónomos que tienen ese carácter porque la Constitución o la ley los han reconocido como tales. Por ejemplo, el Banco Central y la Contraloría General de la República son organismos que gozan de autonomía constitucional, el Consejo para la Transparencia y el Instituto Nacional de Derechos Humanos son organismo que gozan de autonomía legal.

[497] Sobre la ausencia de tutela, conviene decir que, en el ordenamiento jurídico chileno, esta es una característica que tienen los órganos de la administración descentralizada, como las municipalidades o las empresas del Estado, que se expresa en que los órganos descentralizados no dependen directamente del Presidente de la República, quien, por consiguiente, no es su superior directo e inmediato, el cual se relaciona con dichos organismos a través del respectivo ministro de Estado.

> *debe tener su propio personal, seleccionado por esta o por un organismo independiente establecido por el Derecho de los Estados miembros, que esté subordinado exclusivamente al miembro o los miembros de la autoridad de control"*.

Se analizarán cada uno de estos elementos que permiten estructurar la independencia de la que gozan las autoridades de control para el tratamiento de datos de carácter personal.

Elementos que estructuran la independencia de los miembros o integrantes de la Autoridad de Control

El artículo 53 del RGPD en su apartado 1 establece que "*Los Estados miembros dispondrán que cada integrante de sus autoridades de control sea nombrado mediante un procedimiento transparente por: - su Parlamento, - su Gobierno, - su Jefe de Estado, o - un organismo independiente encargado del nombramiento en virtud del Derecho de los Estados miembros*".

El RGPD determina que debe existir una Autoridad de control en cada uno de los Estados miembros de la Unión, lo que es obligatorio y vinculante. Como es lógico, cada Estado, dependiendo de su propia estructura institucional determinará quién y cómo se designa dicha autoridad, por cuanto ello es expresión de la soberanía de cada Estado. Sin embargo, no es baladí quién, y cómo se designa a la Autoridad de Control, ya que ello evidentemente influirá en su mayor o menor grado de independencia, pareciendo adecuado una designación mixta o compleja en que no sea solo el gobierno o un único órgano el que designe a la Autoridad de control[498].

Luego, el apartado 2 del artículo 53 y la letra b) del apartado 1 del artículo 54[499] se refieren a los requisitos para ser designado miembro de la Autoridad de control, al señalar la primera disposición:

> "*Cada miembro poseerá la titulación, la experiencia y las aptitudes, en particular en el ámbito de la protección de datos personales, necesarias para el cumplimiento de sus funciones y el ejercicio de sus poderes"*.

Por consiguiente, para ser integrante de una Autoridad de control no solo se requiere el respectivo título, cuestión más objetiva a considerar, sino además se exige la experiencia y aptitudes necesarias, cuestiones del todo relativas, que son difíciles de objetivar y que dan evidentemente un amplio margen de discrecionalidad. Sin embargo, como ya se ha señalado, no solo es compleja la designación de una autoridad de control, también resulta difícil, en la práctica, determinar con exactitud la experiencia y aptitudes requeridas para integrar dicho organismo, un mecanismo formal previamente establecido para su selección determinado por cada Estado miembro sería un buen instrumento para disminuir al máximo las eventuales arbitrariedades que pudieren producirse.

---

[498] Por ejemplo, volviendo nuevamente al sistema chileno, el Contralor General de la República es designado por el Presidente de la República, previa votación favorable de las 3/5 partes de los Senadores en ejercicio. O los consejeros del Consejo para la Transparencia, que son designados por el Presidente de la República, previa ratificación del Senado.

[499] "las cualificaciones y condiciones de idoneidad necesarias para ser nombrado miembro de cada autoridad de control".

La inamovilidad es otra expresión de la independencia de los integrantes de la Autoridad de Control relacionada con la duración del tiempo en que integrarán el respectivo órgano de control, así el RGPD establece el periodo mínimo de duración para integrar las o la Autoridad de control en la letra d) del apartado 1 del artículo 54 al señalar: "la duración del mandato del miembro o los miembros de cada autoridad de control, no inferior a cuatro años, salvo el primer nombramiento posterior al 24 de mayo de 2016, parte del cual podrá ser más breve cuando sea necesario para proteger la independencia de la autoridad de control por medio de un procedimiento de nombramiento escalonado".

Evidentemente este periodo puede ser mayor, ya que esto queda en el ámbito de la soberanía de cada Estado, dejando abierta la posibilidad de una renovación.[500]

Relacionado igualmente con los plazos en que ejercerán sus mandatos se encuentra el apartado 3 del artículo 53 que señala: "Los miembros darán por concluidas sus funciones en caso de terminación del mandato, dimisión o jubilación obligatoria, de conformidad con el Derecho del Estado miembro de que se trate".

También la independencia de los miembros de la Autoridad de control se expresa en su inamovilidad la que se desprende de la expresión "únicamente" a la que se refiere el apartado 4 del artículo 53, que señala: "Un miembro será destituido únicamente en caso de conducta irregular grave o si deja de cumplir las condiciones exigidas en el desempeño de sus funciones". Si bien la Directiva 95/46/CE no se refería a ella, si lo hizo el Tribunal de Justicia de la Unión Europea TJUE en el Asunto C-288/12 Comisión/Hungría, en sus considerandos 38 y 55. En el considerando 38 dispuso: "La Comisión y el SEPD reconocen que la Directiva 95/46 concede un margen de maniobra a los Estados miembros por lo que respecto a la aplicación de su artículo 28, en particular por lo que se refiere a la elección del modelo institucional y a la duración precisa del mandato de la autoridad de control. Por consiguiente, los Estados miembros pueden en principio determinar libremente esa duración. No obstante, una vez que se ha definido la duración de ese mandato, el Estado miembro debe respetarlo y no puede poner fin al mismo antes de tiempo salvo que concurran motivos graves y comprobables objetivamente. A juicio de la Comisión y el SEPD, confirma esta interpretación, una comparación con el artículo 42 del Reglamento N° 45/2001, relativo al SEPD". Y luego el considerando 55 de la misma sentencia señaló: "Además, en tal situación, no cabría considerar que la autoridad de control pueda actuar, en cualquier circunstancia, por encima de toda sospecha de parcialidad. Así pues, debe interpretarse necesariamente que la exigencia de independencia contenida en el artículo 28, apartado 1, párrafo segundo, de la Directiva 95/46 incluye la obligación de respetar la duración del mandato de las autoridades de control hasta su expiración y de poner fin antes de tiempo al mismo únicamente cuando se observen las normas y las garantías de la legislación aplicable".

Finalmente, en lo que respecta a los elementos que configuran la independencia de los miembros de la autoridad de control, se encuentra las denominadas "incompatibilidades" a las que se refiere el apartado 3 del artículo 52, al señalar: "El miembro o los miembros de cada autoridad de control se abstendrán de cualquier acción que sea incompatible con sus funciones

[500] El Artículo 54 1. Letra e) señala: "el carácter renovable o no del mandato del miembro o los miembros de cada autoridad de control y, en su caso, el número de veces que podrá renovarse".

y no participarán, mientras dure su mandato, en ninguna actividad profesional que sea incompatible, remunerada o no".

Como ocurre con los mecanismos de designación de los integrantes de la autoridad de control o el máximo de tiempo en que podrán ejercer sus funciones o la renovación indefinida o no de sus funciones, el Reglamento entrega a cada Estado miembro la regulación de las incompatibilidades para el ejercicio de su cargo, siendo estos los que determinen las prohibiciones relativas a acciones, ocupaciones y prestaciones incompatibles con el cargo durante el mandato y después del mismo.

También los integrantes de la Autoridad de control están sometidos al deber de secreto profesional, alcanzando incluso el periodo posterior al ejercicio de sus funciones como se establece en el apartado 2 del artículo 54 del RGPD, que dispone:

> "*El miembro o miembros y el personal de cada autoridad de control estarán sujetos, de conformidad con el Derecho de la Unión o de los Estados miembros, al deber de secreto profesional, tanto durante su mandato como después del mismo, con relación a las informaciones confidenciales de las que hayan tenido conocimiento en el cumplimiento de sus funciones o el ejercicio de sus poderes. Durante su mandato, dicho deber de secreto profesional se aplicará en particular a la información recibida de personas físicas en relación con infracciones del presente Reglamento"*.

Este deber de secreto ya estaba establecido en la anterior Directiva 95/46/CE, en el apartado 7 del artículo 28[501].

Elementos que estructuran la independencia en el funcionamiento de la Autoridad de Control

Estos elementos están relacionados con aspectos vinculados a recursos humanos, financieros y presupuestarios, es decir, con la infraestructura humana y material con la que deben contar para el ejercicio de sus atribuciones la o las Autoridades de control. En definitiva, con aspectos vinculados a la forma de organizarse y desarrollar su gestión. En este sentido, el considerando 120 del RGPD dispone que:

> "*Todas las autoridades de control deben estar dotadas de los recursos financieros y humanos, los locales y las infraestructuras que sean necesarios para la realización eficaz de sus funciones, en particular las relacionadas con la asistencia recíproca y la cooperación con otras autoridades de control de la Unión. Cada autoridad de control debe disponer de un presupuesto anual público propio, que podrá formar parte del presupuesto general del Estado o de otro ámbito nacional"*.

De igual forma el apartado 4 del artículo 52 del Reglamento se refiere a esto al señalar:

> "*Cada Estado miembro garantizará que cada autoridad de control disponga en todo momento de los recursos humanos, técnicos y financieros, así como de los locales y las infraestructuras necesarios para el cumplimiento efectivo de sus funciones y el*

[501] "Los Estados miembros dispondrán que los miembros y agentes de las autoridades de control estarán sujetos, incluso después de haber cesado en sus funciones, al deber de secreto profesional sobre informaciones confidenciales a las que hayan tenido acceso".

> *ejercicio de sus poderes, incluidos aquellos que haya de ejercer en el marco de la asistencia mutua, la cooperación y la participación en el Comité"*.

En definitiva, el Reglamento tanto en sus considerandos como en sus disposiciones establece la posibilidad de que existan una o más autoridades de control, las que deben disponer de recursos humanos y materiales para el adecuado ejercicio de tutelar la protección de datos de carácter personal, para lo cual los Estados contarán con las partidas presupuestarias respectivas. Disponiendo además que debe existir una adecuada cooperación y asistencia mutua entre dichas autoridades.

Sobre la autonomía del personal, del considerando 121 del RGPD se desprende que la Autoridad de control debe tener su propio personal, pudiendo ser seleccionado por el propio organismo o por otro independiente establecido por el Derecho de los Estados miembros. Asimismo, el apartado 5 del artículo 52 dispone que:

> "*Cada Estado miembro garantizará que cada autoridad de control elija y disponga de su propio personal, que estará sujeto a la autoridad exclusiva del miembro o miembros de la autoridad de control interesada"*.

Es decir, el proceso de selección de los integrantes de la Autoridad de control debe ser autónomo e independiente para evitar o disminuir potenciales injerencias de todo otro organismo o autoridad, como también para impedir potenciales conflictos de interés en el desempeño de sus funciones, entregando la supervisión o jerarquía directa de cada integrante a la respectiva Autoridad de Control en materia de protección de datos, de manera exclusiva y excluyente.

Luego, sobre la autonomía presupuestaria y financiera se refiere el apartado 6 del artículo 52, que señala:

> "*Cada Estado miembro garantizará que cada autoridad de control esté sujeta a un control financiero que no afecte a su independencia y que disponga de un presupuesto anual, público e independiente, que podrá formar parte del presupuesto general del Estado o de otro ámbito nacional"*.

Esta autonomía o independencia financiera no afecta sin embargo al respectivo control, cuestión que se refuerza en el considerando 118 del RGPD, que dispone:

> "*La independencia de las autoridades de control no debe significar que dichas autoridades puedan quedar exentas de mecanismos de control o supervisión en relación con sus gastos financieros, o de control judicial"*.

De esta forma, el RGPD asume que la Autoridad de Control estando afecta a control financiero no pierde o disminuye en nada su independencia[502].

Lo anterior es propio de un Estado de derecho en que sus distintos organismos e instituciones están afectos a controles recíprocos, en especial si se trata de recursos públicos, donde tanto los ingresos como los gastos deben dirigirse a los objetivos previamente definidos y autorizados por la correspondiente autoridad, debiendo posteriormente rendir cuenta de estos.

[502] Mitjans Perelló, E. (2014), "Los desafíos y la experiencia de la Autoridad Catalana de protección de datos (2005-2012)", *Régimen jurídico de los derechos personales*. Abelado Perrot. Buenos Aires, Argentina.

Competencia, Funciones y Poderes de la Autoridad de Control

En la Sección dos del capítulo seis, entre los artículos 55 y 58, el RGPD se refiere a la competencia, funciones y poderes de la Autoridad de control. Materia que si bien ya se abordaba en la Directiva 95/46/CE, no era uniforme en todos los Estados miembros, especialmente en lo que decía relación con la regulación de sus facultades de fiscalización y en su capacidad coercitiva, señalaba el considerando 63 de la Directiva que "…dicha autoridad debe disponer de los medios necesarios para cumplir su función, ya se trate de poderes de investigación o de intervención, en particular en casos de reclamaciones presentadas a la autoridad o de poder comparecer en juicio; que tal autoridad ha de contribuir a la transparencia de los tratamientos de datos efectuados en el Estado miembro del que dependa".

Esta disparidad también se expresaba en las facultades inspectoras y en la entidad de las sanciones que podía imponer. Ya se refería a ello Troncoso Reigada, en el año 2003, cuando señalaba: "La mayoría de las Autoridades de Control de países de la Unión Europea – a excepción de España y Portugal – suelen tener un nivel de teorización bastante elevado sobre el derecho fundamental a la protección de datos personales – especialmente la Autoridad francesa e italiana -, que no se ve refrendado ni por el contenido de las legislaciones de estos países, ni por las potestades que éstas atribuyen a la Autoridad de Control, ni por la actividad de inspección y sanción, que no llevan a cabo en realidad. Y aunque tengan estos poderes, no los ejercen por sus tradiciones jurídicas. La Autoridad alemana, además de estar encuadrada en el Ministerio del Interior, no desarrolla una labor real de inspección. La Autoridad italiana elige los temas que investiga y solo lleva a cabo inspecciones puntuales. La Autoridad francesa hace básicamente deliberaciones, pero tampoco lleva a cabo inspecciones realmente. No obstante, la Comisión francesa tiene un importante poder político al ser sus miembros diputados. La Agencia de Gran Bretaña tiene que pedir permiso para hacer una inspección al responsable del fichero – orden de *enforcement* -. Si el responsable se niega, solo le queda ir a los Tribunales. La Agencia irlandesa ha hecho una sola inspección en los últimos cinco años. Solo Portugal y Grecia atribuyen poderes reales de inspección en materia de protección de datos, lo que no es decir mucho. En pocos ámbitos se ve tanta incongruencia entre lo que se predica en los foros internacionales y lo que efectivamente se lleva a cabo en los respectivos países. No existe realmente una tutela efectiva del derecho fundamental a la protección de datos en el ámbito europeo"[503].

Si bien son discutibles estas afirmaciones, especialmente mirándolas desde el contexto latinoamericano, lo cierto es que el Reglamento avanza ostensiblemente en una mayor coherencia, y contribuye a uniformar las capacidades y facultades de la Autoridad de control en materia de protección de datos en toda Europa.

Competencia

A la competencia de la Autoridad de Control se refieren los artículos 55 y 56 del Reglamento, el artículo 55 dispone que:

[503] Troncoso Reigada, A. (2003), "La protección de datos personales. Una reflexión crítica de la jurisprudencia constitucional", *Cuadernos de Derecho Público* n° 19-20, pp. 314-315.

"1. Cada autoridad de control será competente para desempeñar las funciones que se le asignen y ejercer los poderes que se le confieran de conformidad con el presente Reglamento en el territorio de su Estado miembro. 2. Cuando el tratamiento sea efectuado por autoridades públicas o por organismos privados que actúen con arreglo al artículo 6, apartado 1, letras c) o e), será competente la autoridad de control del Estado miembro de que se trate. No será aplicable en tales casos el artículo 56. 3. Las autoridades de control no serán competentes para controlar las operaciones de tratamiento efectuadas por los tribunales en el ejercicio de su función judicial".

El apartado uno de la precedente disposición está relacionado con el ámbito de aplicación tanto material como territorial del RGPD, que están delimitados en sus artículos 2 y 3 respectivamente. Si bien su ámbito de aplicación material es amplio, se excluyen de su regulación el tratamiento de datos de las personas jurídicas, de las personas fallecidas, así como la información anonimizada, disociada de datos personales.

Artículo 2; "Ámbito de aplicación material 1. El presente Reglamento se aplica al tratamiento total o parcialmente automatizado de datos personales, así como al tratamiento no automatizado de datos personales contenidos o destinados a ser incluidos en un fichero. 2. El presente Reglamento no se aplica al tratamiento de datos personales: a) en el ejercicio de una actividad no comprendida en el ámbito de aplicación del Derecho de la Unión; b) por parte de los Estados miembros cuando lleven a cabo actividades comprendidas en el ámbito de aplicación del capítulo 2 del título V del TUE; c) efectuado por una persona física en el ejercicio de actividades exclusivamente personales o domésticas; d) por parte de las autoridades competentes con fines de prevención, investigación, detección o enjuiciamiento de infracciones penales, o de ejecución de sanciones penales, incluida la de protección frente a amenazas a la seguridad pública y su prevención. 3. El Reglamento (CE) n.o 45/2001 es de aplicación al tratamiento de datos de carácter personal por parte de las instituciones, órganos y organismos de la Unión. El Reglamento (CE) n.o 45/2001 y otros actos jurídicos de la Unión aplicables a dicho tratamiento de datos de carácter personal se adaptarán a los principios y normas del presente Reglamento de conformidad con su artículo 98. 4. El presente Reglamento se entenderá sin perjuicio de la aplicación de la Directiva 2000/31/CE, en particular sus normas relativas a la responsabilidad de los prestadores de servicios intermediarios establecidas en sus artículos 12 a 15".

Artículo 3; "Ámbito territorial 1. El presente Reglamento se aplica al tratamiento de datos personales en el contexto de las actividades de un establecimiento del responsable o del encargado en la Unión, independientemente de que el tratamiento tenga lugar en la Unión o no. L 119/32 ES Diario Oficial de la Unión Europea 4.5.2016 2. El presente Reglamento se aplica al tratamiento de datos personales de interesados que residan en la Unión por parte de un responsable o encargado no establecido en la Unión, cuando las actividades de tratamiento estén relacionadas con: a) la oferta de bienes o servicios a dichos interesados en la Unión, independientemente de si a estos se les requiere su pago, o b) el control de su comportamiento, en la medida en que este tenga lugar en la Unión. 3. El presente Reglamento se aplica al tratamiento de datos personales por parte de un responsable que no esté establecido en la Unión sino en un

> *lugar en que el Derecho de los Estados miembros sea de aplicación en virtud del Derecho internacional público".*

En relación al apartado dos del artículo 55, se desprende que cuando el tratamiento sea efectuado por autoridades públicas o por organismos privados que actúen para el cumplimiento de una obligación legal aplicable al responsable del tratamiento, o el tratamiento es necesario para el cumplimiento de una misión realizada en interés público, o en el ejercicio de poderes públicos conferidos al responsable del tratamiento, será competente la autoridad de control del Estado miembro de que se trate, sin que le sean aplicables las disposiciones contenidas en el artículo 56 del Reglamento.

Asimismo, el apartado tres dispone que las autoridades de control no tienen competencia para regular y controlar el tratamiento de datos que realicen los tribunales de justicia en el ejercicio de su función jurisdiccional. Esta disposición resulta del todo coherente por cuanto la autoridad de control no puede regular las actuaciones de los órganos jurisdiccionales, considerando que sus actuaciones, las de la autoridad de control, pueden luego ser impugnadas o recurridas ante dichos tribunales. Además, el propio RGPD refuerza esta idea en su considerando 20, al señalar:

> *"Aunque el presente Reglamento se aplica, entre otras, a las actividades de los tribunales y otras autoridades judiciales, en virtud del Derecho de la Unión o de los Estados miembros pueden especificarse las operaciones de tratamiento y los procedimientos de tratamiento en relación con el tratamiento de datos personales por los tribunales y otras autoridades judiciales. A fin de preservar la independencia del poder judicial en el desempeño de sus funciones, incluida la toma de decisiones, la competencia de las autoridades de control no debe abarcar el tratamiento de datos personales cuando los tribunales actúen en ejercicio de su función judicial. El control de esas operaciones de tratamiento de datos ha de poder encomendarse a organismos específicos establecidos dentro del sistema judicial del Estado miembro, los cuales deben, en particular, garantizar el cumplimiento de las normas del presente Reglamento, concienciar más a los miembros del poder judicial acerca de sus obligaciones en virtud de este y atender las reclamaciones en relación con tales operaciones de tratamiento de datos".*

En el caso español, el tratamiento de datos que realizan los tribunales de justicia es regulado por el Consejo General del Poder Judicial[504]. Así también lo señala Delgado Martín "en la normativa vigente española, el Consejo General del Poder Judicial es la Autoridad de control en relación con los ficheros jurisdiccionales y los tratamientos aplicados a los mismo, ejerciendo las competencias que la normativa general de protección de datos atribuye a la Agencia Española de Protección de Datos"[505].

[504] Según el apartado tres del Artículo 44 de la Ley Orgánica 3/2018 de protección de datos y garantía de los derechos digitales que dispone: "La Agencia Española de Protección de Datos y el Consejo General del Poder Judicial colaborarán en aras del adecuado ejercicio de las respectivas competencias que la Ley Orgánica 6/1985, de 1 julio, del Poder Judicial, les atribuye en materia de protección de datos personales en el ámbito de la Administración de Justicia".

[505] Delgado Martín, J. (2019), "Reflexiones sobre la protección de datos personales en la Administración de Justicia", *Diario La Ley*, n° 9326, sección Tribuna, 21 de febrero, p.9.

A continuación, el artículo 56 del RGPD se refiere a la competencia de la autoridad de control principal y al tratamiento transfronterizo de datos, al señalar:

"*Competencia de la autoridad de control principal*

1. Sin perjuicio de lo dispuesto en el artículo 55, la autoridad de control del establecimiento principal o del único establecimiento del responsable o del encargado del tratamiento será competente para actuar como autoridad de control principal para el tratamiento transfronterizo realizado por parte de dicho responsable o encargado con arreglo al procedimiento establecido en el artículo 60.

2. No obstante lo dispuesto en el apartado 1, cada autoridad de control será competente para tratar una reclamación que le sea presentada o una posible infracción del presente Reglamento, en caso de que se refiera únicamente a un establecimiento situado en su Estado miembro o únicamente afecte de manera sustancial a interesados en su Estado miembro.

3. En los casos a que se refiere el apartado 2 del presente artículo, la autoridad de control informará sin dilación al respecto a la autoridad de control principal. En el plazo de tres semanas después de haber sido informada, la autoridad de control principal decidirá si tratará o no el caso de conformidad con el procedimiento establecido en el artículo 60, teniendo presente si existe un establecimiento del responsable o encargado del tratamiento en el Estado miembro de la autoridad de control que le haya informado.

4. En caso de que la autoridad de control principal decida tratar el caso, se aplicará el procedimiento establecido en el artículo 60. La autoridad de control que haya informado a la autoridad de control principal podrá presentarle un proyecto de decisión. La autoridad de control principal tendrá en cuenta en la mayor medida posible dicho proyecto al preparar el proyecto de decisión a que se refiere el artículo 60, apartado 3.

5. En caso de que la autoridad de control principal decida no tratar el caso, la autoridad de control que le haya informado lo tratará con arreglo a los artículos 61 y 62.

6. La autoridad de control principal será el único interlocutor del responsable o del encargado en relación con el tratamiento transfronterizo realizado por dicho responsable o encargado".

El Reglamento también refuerza la competencia que tiene cada autoridad de control en su respectivo Estado y establece que dichas autoridades de control deben regular también la transferencia de datos personales entre los Estados de la Unión de conformidad al Reglamento, para que se aplique coherentemente, lo que requiere coordinación y cooperación recíproca entre las mismas.

En este mismo sentido el considerando 123 del RGPD dispone:

> *"A fin de proteger a las personas físicas con respecto al tratamiento de sus datos personales y de facilitar la libre circulación de los datos personales en el mercado interior, las autoridades de control deben supervisar la aplicación de las disposiciones adoptadas de conformidad con el presente Reglamento y contribuir a su aplicación coherente en toda la Unión. A tal efecto, las autoridades de control deben cooperar entre ellas y con la Comisión, sin necesidad de acuerdo alguno entre Estados miembros sobre la prestación de asistencia mutua ni sobre dicha cooperación".*

De lo anterior también se desprende que cuando exista un establecimiento principal, por cuanto el responsable o encargado del tratamiento está establecido en más de un Estado, será responsable la autoridad de control donde dicho establecimiento principal esté ubicado, constituyéndose dicha autoridad, como la autoridad de control principal. Lo mismo ocurrirá cuando el tratamiento afecte o potencialmente lo haga, a interesados o titulares de más de un Estado miembro, aun cuando el establecimiento que trata los datos sea único.

El numeral 16 del Artículo 4 del RGPD señala que:

> "*el establecimiento principal: a) en lo que se refiere a un responsable del tratamiento con establecimientos en más de un Estado miembro, el lugar de su administración central en la Unión, salvo que las decisiones sobre los fines y los medios del tratamiento se tomen en otro establecimiento del responsable en la Unión y este último establecimiento tenga el poder de hacer aplicar tales decisiones, en cuyo caso el establecimiento que haya adoptado tales decisiones se considerará establecimiento principal; b) en lo que se refiere a un encargado del tratamiento con establecimientos en más de un Estado miembro, el lugar de su administración central en la Unión o, si careciera de esta, el establecimiento del encargado en la Unión en el que se realicen las principales actividades de tratamiento en el contexto de las actividades de un establecimiento del encargado en la medida en que el encargado esté sujeto a obligaciones específicas con arreglo al presente Reglamento*".

La autoridad de control principal debe, entonces, coordinarse y cooperar, con todas las otras autoridades de control involucradas en el tratamiento de datos de carácter personal.

Si la reclamación no se presenta ante la autoridad de control principal, ésta igualmente debe cooperar con la autoridad de control ante la cual se presentó la solicitud, la cual opera como "ventanilla única", y seguirá siendo competente para realizar cualquier investigación en el territorio de su propio Estado, tal como se establece en el considerando 130 del Reglamento.

> *Considerando 130 RGPD; "Cuando la autoridad de control ante la cual se haya presentado la reclamación no sea la autoridad de control principal, esta última debe cooperar estrechamente con la primera con arreglo a las disposiciones sobre cooperación y coherencia establecidas en el presente Reglamento. En tales casos, la autoridad de control principal, al tomar medidas concebidas para producir efectos jurídicos, incluida la imposición de multas administrativas, debe tener en cuenta en la mayor medida posible la opinión de la autoridad de control ante la cual se haya presentado la reclamación y la cual debe seguir siendo competente para realizar cualquier investigación en el territorio de su propio Estado miembro en enlace con la autoridad de control competente".*

De igual forma, y según se colige del RGPD, cuando el titular o interesado no resida en el Estado miembro donde presenta una reclamación, la autoridad de control de dicho Estado se convierte en la autoridad de control interesada[506].

[506] El artículo 4. 22 define a la autoridad interesada; "autoridad de control interesada": la autoridad de control a la que afecta el tratamiento de datos personales debido a que: a) el responsable o el encargado del tratamiento está establecido en el territorio del Estado miembro de esa autoridad de control; b) los interesados que residen en el

Otro aspecto interesante relacionado con el tratamiento transfronterizo de datos, es que el Reglamento promueve un "arreglo amistoso", expresión también del principio de cooperación, pero en este caso entre la autoridad de control y el responsable del tratamiento, en las condiciones que lo señala el considerando 131:

"En casos en los que otra autoridad de control deba actuar como autoridad de control principal para las actividades de tratamiento del responsable o del encargado pero el objeto concreto de una reclamación o la posible infracción afecta únicamente a las actividades de tratamiento del responsable o del encargado en el Estado miembro en el que se haya presentado la reclamación o detectado la posible infracción y el asunto no afecta sustancialmente ni es probable que afecte sustancialmente a interesados de otros Estados miembros, la autoridad de control que reciba una reclamación o que detecte situaciones que conlleven posibles infracciones del presente Reglamento o reciba de otra manera información sobre estas debe tratar de llegar a un arreglo amistoso con el responsable del tratamiento y, si no prospera, ejercer todos sus poderes. En lo anterior se debe incluir el tratamiento específico realizado en el territorio del Estado miembro de la autoridad de control o con respecto a interesados en el territorio de dicho Estado miembro; el tratamiento efectuado en el contexto de una oferta de bienes o servicios destinada específicamente a interesados en el territorio del Estado miembro de la autoridad de control; o el tratamiento que deba evaluarse teniendo en cuenta las obligaciones legales pertinentes en virtud del Derecho de los Estados miembros".

Asimismo, la autoridad de control que no es la principal goza de competencia para tratar asuntos locales cuando el objeto del tratamiento se refiere exclusivamente a un único Estado miembro y afecta a interesados de ese mismo único Estado, aun cuando el encargado o responsable del tratamiento está establecido en más de un Estado miembro[507].

Por último, en lo referido la competencia de la Autoridad de control, es importante señalar que el mecanismo de "ventanilla única" al que se ha hecho referencia y que regula el RGPD, no opera cuando el tratamiento se realiza por autoridades públicas u organismos privados en

Estado miembro de esa autoridad de control se ven sustancialmente afectados o es probable que se vean sustancialmente afectados por el tratamiento, o c) se ha presentado una reclamación ante esa autoridad de control".

[507] Así se desprende del considerando 127 del RGPD: "Cada autoridad de control que no actúa como autoridad principal debe ser competente para tratar asuntos locales en los que, si bien el responsable o el encargado del tratamiento está establecido en más de un Estado miembro, el objeto del tratamiento específico se refiere exclusivamente al tratamiento efectuado en un único Estado miembro y afecta exclusivamente a interesados de ese único Estado miembro, por ejemplo cuando el tratamiento tiene como objeto datos personales de empleados en el contexto específico de empleo de un Estado miembro. En tales casos, la autoridad de control debe informar sin dilación al respecto a la autoridad de control principal. Una vez informada, la autoridad de control principal debe decidir si tratará el asunto de acuerdo con la disposición aplicable a la cooperación entre la autoridad de control principal y otras autoridades de control interesadas («mecanismo de ventanilla única»), o si lo debe tratar localmente la autoridad de control que le haya informado. Al decidir si trata el asunto, la autoridad de control principal debe considerar si existe un establecimiento del responsable o del encargado en el Estado miembro de la autoridad de control que le haya informado, con el fin de garantizar la ejecución efectiva de la decisión respecto del responsable o encargado del tratamiento. Si la autoridad de control principal decide tratar el asunto, se debe ofrecer a la autoridad de control informante de la posibilidad de presentar un proyecto de decisión, que la autoridad de control principal ha de tener en cuenta en la mayor medida posible al preparar su proyecto de decisión al amparo del mecanismo de ventanilla única".

interés público, siendo competente la autoridad de control del Estado donde estén establecidas dicha autoridad u organismo privado.

Funciones

A las funciones de la autoridad de control se refiere en extenso el artículo 57 del Reglamento, que señala:

Sin perjuicio de otras funciones en virtud del presente Reglamento, incumbirá a cada autoridad de control, en su territorio:

- *controlar la aplicación del presente Reglamento y hacerlo aplicar;*
- *promover la sensibilización del público y su comprensión de los riesgos, normas, garantías y derechos en relación con el tratamiento. Las actividades dirigidas específicamente a los niños deberán ser objeto de especial atención;*
- *asesorar, con arreglo al Derecho de los Estados miembros, al Parlamento nacional, al Gobierno y a otras instituciones y organismos sobre las medidas legislativas y administrativas relativas a la protección de los derechos y libertades de las personas físicas con respecto al tratamiento;*
- *promover la sensibilización de los responsables y encargados del tratamiento acerca de las obligaciones que les incumben en virtud del presente Reglamento;*
- *previa solicitud, facilitar información a cualquier interesado en relación con el ejercicio de sus derechos en virtud del presente Reglamento y, en su caso, cooperar a tal fin con las autoridades de control de otros Estados miembros;*
- *tratar las reclamaciones presentadas por un interesado o por un organismo, organización o asociación de conformidad con el artículo 80, e investigar, en la medida oportuna, el motivo de la reclamación e informar al reclamante sobre el curso y el resultado de la investigación en un plazo razonable, en particular si fueran necesarias nuevas investigaciones o una coordinación más estrecha con otra autoridad de control;*
- *cooperar, en particular compartiendo información, con otras autoridades de control y prestar asistencia mutua con el fin de garantizar la coherencia en la aplicación y ejecución del presente Reglamento;*
- *llevar a cabo investigaciones sobre la aplicación del presente Reglamento, en particular basándose en información recibida de otra autoridad de control u otra autoridad pública;*
- *hacer un seguimiento de cambios que sean de interés, en la medida en que tengan incidencia en la protección de datos personales, en particular el desarrollo de las tecnologías de la información y la comunicación y las prácticas comerciales;*
- *adoptar las cláusulas contractuales tipo a que se refieren el artículo 28, apartado 8, y el artículo 46, apartado 2, letra d);*
- *elaborar y mantener una lista relativa al requisito de la evaluación de impacto relativa a la protección de datos, en virtud del artículo 35, apartado 4;*
- *ofrecer asesoramiento sobre las operaciones de tratamiento contempladas en el artículo 36, apartado 2;*

- *alentar la elaboración de códigos de conducta con arreglo al artículo 40, apartado 1, y dictaminar y aprobar los códigos de conducta que den suficientes garantías con arreglo al artículo 40, apartado 5;*
- *fomentar la creación de mecanismos de certificación de la protección de datos y de sellos y marcas de protección de datos con arreglo al artículo 42, apartado 1, y aprobar los criterios de certificación de conformidad con el artículo 42, apartado 5;*
- *llevar a cabo, si procede, una revisión periódica de las certificaciones expedidas en virtud del artículo 42, apartado 7;*
- *elaborar y publicar los criterios para la acreditación de organismos de supervisión de los códigos de conducta con arreglo al artículo 41 y de organismos de certificación con arreglo al artículo 43;*
- *efectuar la acreditación de organismos de supervisión de los códigos de conducta con arreglo al artículo 41 y de organismos de certificación con arreglo al artículo 43;*
- *autorizar las cláusulas contractuales y disposiciones a que se refiere el artículo 46, apartado 3;*
- *aprobar normas corporativas vinculantes de conformidad con lo dispuesto en el artículo 47;*
- *contribuir a las actividades del Comité;*
- *llevar registros internos de las infracciones del presente Reglamento y de las medidas adoptadas de conformidad con el artículo 58, apartado 2; y*
- *desempeñar cualquier otra función relacionada con la protección de los datos personales.*

Cada autoridad de control facilitará la presentación de las reclamaciones contempladas en el apartado 1, letra f) mediante medidas como un formulario de presentación de reclamaciones que pueda cumplimentarse también por medios electrónicos, sin excluir otros medios de comunicación.

El desempeño de las funciones de cada autoridad de control será gratuito para el interesado y, en su caso, para el delegado de protección de datos.

Cuando las solicitudes sean manifiestamente infundadas o excesivas, especialmente debido a su carácter repetitivo, la autoridad de control podrá establecer una tasa razonable basada en los costes administrativos o negarse a actuar respecto de la solicitud. La carga de demostrar el carácter manifiestamente infundado o excesivo de la solicitud recaerá en la autoridad de control.

Del extenso catálogo de funciones al que se refiere el apartado uno del artículo 57 del RGPD, la letra a) es la de mayor importancia, ya que se refiere a la principal función de la autoridad de control, que no es otra que cumplir y hacer cumplir las disposiciones en él contenidas, lo que resulta armónico con el objeto del Reglamento previsto en su artículo primero[508], que es

[508] "Objeto 1. El presente Reglamento establece las normas relativas a la protección de las personas físicas en lo que respecta al tratamiento de los datos personales y las normas relativas a la libre circulación de tales datos. 2.

en lo sustancial regular la protección y los derechos y libertades de las personas físicas en lo que respecta al tratamiento de los datos personales y las normas relativas a la libre circulación de tales datos.

Este conjunto de funciones es posible sistematizarlo, para lo cual, y siguiendo a Troncoso Reigada, se pueden distinguir: a) funciones coercitivas o de ejercicio del poder público; b) funciones de prestación y promoción del derecho a la protección de datos personales; y c) funciones de cooperación con otras autoridades de control[509].

a) Las Funciones coercitivas

Son propias de la autoridad administrativa en el ejercicio del poder público, e implican la función de investigación sobre el cumplimiento de legislación de parte de los responsables y encargados del tratamiento. Esta función de investigación puede iniciarse por dos vías: por una reclamación ante la autoridad de control y de oficio o a instancia de otra autoridad de control.

En el primer caso, esto es, por la presentación de una reclamación ante la autoridad de control, le corresponde a esta última abocarse a las reclamaciones presentadas en su territorio por un interesado, organismo, organización o asociación, según el artículo 80 del RGPD, e investigar, en la medida oportuna, el motivo de la reclamación e informar al reclamante sobre el curso y el resultado de la investigación en un plazo razonable, en particular si fueran necesarias nuevas investigaciones o una coordinación más estrecha con otra autoridad de control[510].

Artículo 80 del RGPD;

"*Representación de los interesados*

1. El interesado tendrá derecho a dar mandato a una entidad, organización o asociación sin ánimo de lucro que haya sido correctamente constituida con arreglo al Derecho de un Estado miembro, cuyos objetivos estatutarios sean de interés público y que actúe en el ámbito de la protección de los derechos y libertades de los interesados en materia de protección de sus datos personales, para que presente en su nombre la reclamación, y ejerza en su nombre los derechos contemplados en los artículos 77, 78 y 79, y el derecho a ser indemnizado mencionado en el artículo 82 si así lo establece el Derecho del Estado miembro.

2. Cualquier Estado miembro podrán disponer que cualquier entidad, organización o asociación mencionada en el apartado 1 del presente artículo tenga, con independencia del mandato del interesado, derecho a presentar en ese Estado miembro una reclamación ante la autoridad de control que sea competente en virtud del artículo 77 y a ejercer los derechos contemplados en los artículos 78 y 79, si considera que los derechos del interesado con arreglo al presente Reglamento han sido vulnerados como consecuencia de un tratamiento".

El presente Reglamento protege los derechos y libertades fundamentales de las personas físicas y, en particular, su derecho a la protección de los datos personales. 3. La libre circulación de los datos personales en la Unión no podrá ser restringida ni prohibida por motivos relacionados con la protección de las personas físicas en lo que respecta al tratamiento de datos personales".

[509] Troncoso Reigada, A. (2016), "Autoridades de control independientes", en *Reglamento General de Protección de Datos, Hacia un nuevo modelo europeo de privacidad*. Director Piñar Mañas, J., Coordinadores Alvarez Caro, M. y Recio Gayo, M.Reus, Madrid, pp. 498-505.

[510] Artículo 57, apartado 1, letra f).

La autoridad de control está afecta al denominado principio de responsabilidad proactiva, en virtud del cual no solo se limita a recibir la reclamación y dar curso a su tramitación, sino que también promueve y proporciona la presentación de reclamaciones facilitando un formulario de reclamaciones al que se refiere el aparatado dos del artículo 57 del Reglamento:

> "*Cada autoridad de control facilitará la presentación de las reclamaciones contempladas en el apartado 1, letra f), mediante medidas como un formulario de presentación de reclamaciones que pueda cumplimentarse también por medios electrónicos, sin excluir otros medios de comunicación"*.

En el segundo caso, la investigación se inicia de oficio o a petición de otra autoridad de control, según lo dispone la letra h) del apartado 1 del artículo 57 del Reglamento, al señalar que incumbe a cada autoridad de control en su territorio, "llevar a cabo investigaciones sobre la aplicación del presente Reglamento, en particular basándose en información recibida de otra autoridad de control u otra autoridad pública".

Para el desarrollo de esta función coercitiva la autoridad de control debe llevar registros internos de las infracciones al Reglamento y de las medidas adoptadas, las que dicen relación con poderes coercitivos señalados en el apartado dos del artículo 58 del RGPD.

También la función coercitiva le asigna a la autoridad de control la elaboración y mantención de una lista que evalúe el impacto a la protección de datos, cuando un determinado tratamiento que realiza el responsable de estos implique un alto riesgo para los derechos de las personas[511]. Por consiguiente, esta función representa una obligación para el responsable del tratamiento de datos de carácter personal.

La función coercitiva incluye también la autorización que otorga la autoridad de control a las garantías aportadas para las transferencias internacionales, especialmente la aprobación de las normas corporativas vinculantes, en relación con el artículo 47 del RGPD, y la autorización también de las cláusulas contractuales entre el responsable o encargado y el responsable, encargado o destinatario de los datos personales en el tercer país u organización internacional, además de la autorización de las disposiciones que incorporen acuerdos administrativos entre autoridades y organismos públicos, en relación con el artículo 46, apartado tres[512].

Artículo 47 del RGPD;

> "*Normas corporativas vinculantes*

[511] A esta lista se refieren los apartados 4 y 5 del Artículo 35 del RGPD, que respectivamente señalan: "4. La autoridad de control establecerá y publicará una lista de los tipos de operaciones de tratamiento que requieran una evaluación de impacto relativa a la protección de datos de conformidad con el apartado 1. La autoridad de control comunicará esas listas al Comité a que se refiere el artículo 68.

5. La autoridad de control podrá asimismo establecer y publicar la lista de los tipos de tratamiento que no requieren evaluaciones de impacto relativas a la protección de datos. La autoridad de control comunicará esas listas al Comité".

[512] "Siempre que exista autorización de la autoridad de control competente, las garantías adecuadas contempladas en el apartado 1 podrán igualmente ser aportadas, en particular, mediante: a) cláusulas contractuales entre el responsable o el encargado y el responsable, encargado o destinatario de los datos personales en el tercer país u organización internacional, o b) disposiciones que se incorporen en acuerdos administrativos entre las autoridades u organismos públicos que incluyan derechos efectivos y exigibles para los interesados".

1. La autoridad de control competente aprobará normas corporativas vinculantes de conformidad con el mecanismo de coherencia establecido en el artículo 63, siempre que estas: a) sean jurídicamente vinculantes y se apliquen y sean cumplidas por todos los miembros correspondientes del grupo empresarial o de la unión de empresas dedicadas a una actividad económica conjunta, incluidos sus empleados; b) confieran expresamente a los interesados derechos exigibles en relación con el tratamiento de sus datos personales, y c) cumplan los requisitos establecidos en el apartado 2. 2. Las normas corporativas vinculantes mencionadas en el apartado 1 especificarán, como mínimo, los siguientes elementos: a) la estructura y los datos de contacto del grupo empresarial o de la unión de empresas dedicadas a una actividad económica conjunta y de cada uno de sus miembros; b) las transferencias o conjuntos de transferencias de datos, incluidas las categorías de datos personales, el tipo de tratamientos y sus fines, el tipo de interesados afectados y el nombre del tercer o los terceros países en cuestión; c) su carácter jurídicamente vinculante, tanto a nivel interno como externo; d) la aplicación de los principios generales en materia de protección de datos, en particular la limitación de la finalidad, la minimización de los datos, los periodos de conservación limitados, la calidad de los datos, la protección de los datos desde el diseño y por defecto, la base del tratamiento, el tratamiento de categorías especiales de datos personales, las medidas encaminadas a garantizar la seguridad de los datos y los requisitos con respecto a las transferencias ulteriores a organismos no vinculados por las normas corporativas vinculantes; e) los derechos de los interesados en relación con el tratamiento y los medios para ejercerlos, en particular el derecho a no ser objeto de decisiones basadas exclusivamente en un tratamiento automatizado, incluida la elaboración de perfiles de conformidad con lo dispuesto en el artículo 22, el derecho a presentar una reclamación ante la autoridad de control competente y ante los tribunales competentes de los Estados miembros de conformidad con el artículo 79, y el derecho a obtener una reparación, y, cuando proceda, una indemnización por violación de las normas corporativas vinculantes; f) la aceptación por parte del responsable o del encargado del tratamiento establecidos en el territorio de un Estado miembro de la responsabilidad por cualquier violación de las normas corporativas vinculantes por parte de cualquier miembro de que se trate no establecido en la Unión; el responsable o el encargado solo será exonerado, total o parcialmente, de dicha responsabilidad si demuestra que el acto que originó los daños y perjuicios no es imputable a dicho miembro; g) la forma en que se facilita a los interesados la información sobre las normas corporativas vinculantes, en particular en lo que respecta a las disposiciones contempladas en las letras d), e) y f) del presente apartado, además de los artículos 13 y 14; h) las funciones de todo delegado de protección de datos designado de conformidad con el artículo 37, o de cualquier otra persona o entidad encargada de la supervisión del cumplimiento de las normas corporativas vinculantes dentro del grupo empresarial o de la unión de empresas dedicadas a una actividad económica conjunta, así como de la supervisión de la formación y de la tramitación de las reclamaciones; i) los procedimientos de reclamación; j) los mecanismos establecidos dentro del grupo empresarial o de la unión de empresas dedicadas a una actividad económica conjunta para garantizar la verificación del cumplimiento de las normas corporativas vinculantes. Dichos mecanismos incluirán auditorías de protección de datos y métodos para garantizar

> *acciones correctivas para proteger los derechos del interesado. Los resultados de dicha verificación deberían comunicarse a la persona o entidad a que se refiere la letra h) y al consejo de administración de la empresa que controla un grupo empresarial, o de la unión de empresas dedicadas a una actividad económica conjunta, y ponerse a disposición de la autoridad de control competente que lo solicite; k) los mecanismos establecidos para comunicar y registrar las modificaciones introducidas en las normas y para notificar esas modificaciones a la autoridad de control; l) el mecanismo de cooperación con la autoridad de control para garantizar el cumplimiento por parte de cualquier miembro del grupo empresarial o de la unión de empresas dedicadas a una actividad económica conjunta, en particular poniendo a disposición de la autoridad de control los resultados de las verificaciones de las medidas contempladas en la letra j); m) los mecanismos para informar a la autoridad de control competente de cualquier requisito jurídico de aplicación en un país tercero a un miembro del grupo empresarial o de la unión de empresas dedicadas a una actividad económica conjunta, que probablemente tengan un efecto adverso sobre las garantías establecidas en las normas corporativas vinculantes, y n) la formación en protección de datos pertinente para el personal que tenga acceso permanente o habitual a datos personales. La Comisión podrá especificar el formato y los procedimientos para el intercambio de información entre los responsables, los encargados y las autoridades de control en relación con las normas corporativas vinculantes a tenor de lo dispuesto en el presente artículo. Dichos actos de ejecución se adoptarán con arreglo al procedimiento de examen a que se refiere el artículo 93, apartado 2. Artículo 48"*.

El ejercicio de la función coercitiva descrita por las autoridades de control tiene como correlato los poderes establecidos en el artículo 58 del Reglamento, que se abordaran en detalle en las siguientes líneas.

b) Las Funciones de prestación y promoción

Esta función se expresa en las acciones positivas que la autoridad de control debe ejecutar para la plena expresión del derecho a la protección de datos de carácter personal, removiendo los obstáculos que impidan su libre ejercicio. Esta función recae en los encargados, responsables y delegados de protección de datos y en todos los sujetos que sean titulares de ese derecho.

En el marco de esta función, cada autoridad de control debe promover la sensibilización de los responsables y encargados del tratamiento acerca de las obligaciones que les incumben en virtud del Reglamento. De igual forma, esta función de prestación y promoción se expresa en que la autoridad de control debe alentar la elaboración de códigos de conducta con arreglo al artículo 40, apartado 1, y dictaminar y aprobar los códigos de conducta que den suficientes garantías con arreglo al artículo 40, apartado 5.

> *Artículo 40, apartado 1 del RGPD; "Los Estados miembros, las autoridades de control, el Comité y la Comisión promoverán la elaboración de códigos de conducta destinados a contribuir a la cor1recta aplicación del presente Reglamento, teniendo en cuenta las características específicas de los distintos sectores de tratamiento y las necesidades específicas de las microempresas y las pequeñas y medianas empresas"*.

> *Artículo 40, apartado 5 del RGPD; "Las asociaciones y otros organismos mencionados en el apartado 2 del presente artículo que proyecten elaborar un código de conducta o modificar o ampliar un código existente presentarán el proyecto de código o la modificación o ampliación a la autoridad de control que sea competente con arreglo al artículo 55. La autoridad de control dictaminará si el proyecto de código o la modificación o ampliación es conforme con el presente Reglamento y aprobará dicho proyecto de código, modificación o ampliación si considera suficientes las garantías adecuadas ofrecidas".*

Además de fomentar la creación de mecanismos de certificación de la protección de datos y de sellos y marcas de protección de datos con arreglo al artículo 42, apartado 1, y aprobar los criterios de certificación de conformidad con el artículo 42, apartados 5 y 7. Del mismo modo, la autoridad de control en el ejercicio de esta función debe elaborar y publicar los criterios para la acreditación de organismos de supervisión de los códigos de conducta, así como acreditar a tales organismos con arreglo al artículo 41 y 43 del Reglamento.

> *Artículo 42, apartado 1 del RGPD; "Los Estados miembros, las autoridades de control, el Comité y la Comisión promoverán, en particular a nivel de la Unión, la creación de mecanismos de certificación en materia de protección de datos y de sellos y marcas de protección de datos a fin de demostrar el cumplimiento de lo dispuesto en el presente Reglamento en las operaciones de tratamiento de los responsables y los encargados. Se tendrán en cuenta las necesidades específicas de las microempresas y las pequeñas y medianas empresas".*

> *Artículo 42, apartado 5 del RGPD; "La certificación en virtud del presente artículo será expedida por los organismos de certificación a que se refiere el artículo 43 o por la autoridad de control competente, sobre la base de los criterios aprobados por dicha autoridad de conformidad con el artículo 58, apartado 3, o por el Comité de conformidad con el artículo 63. Cuando los criterios sean aprobados por el Comité, esto podrá dar lugar a una certificación común: el Sello Europeo de Protección de Datos".*

> *Artículo 42, apartado 7 del RGPD; "La certificación se expedirá a un responsable o encargado de tratamiento por un período máximo de tres años y podrá ser renovada en las mismas condiciones, siempre y cuando se sigan cumpliendo los requisitos pertinentes. La certificación será retirada, cuando proceda, por los organismos de certificación a que se refiere el artículo 43, o en su caso por la autoridad de control competente, cuando no se cumplan o se hayan dejado de cumplir los requisitos para la certificación".*

> *Artículo 41 del RGPD; "Supervisión de códigos de conducta aprobados 1. Sin perjuicio de las funciones y los poderes de la autoridad de control competente en virtud de los artículos 57 y 58, podrá supervisar el cumplimiento de un código de conducta en virtud del artículo 40 un organismo que tenga el nivel adecuado de pericia en relación con el objeto del código y que haya sido acreditado para tal fin por la autoridad de control competente. 2. El organismo a que se refiere el apartado 1 podrá ser acreditado para supervisar el cumplimiento de un código de conducta si: a) ha*

demostrado, a satisfacción de la autoridad de control competente, su independencia y pericia en relación con el objeto del código; b) ha establecido procedimientos que le permitan evaluar la idoneidad de los responsables y encargados correspondientes para aplicar el código, supervisar el cumplimiento de sus disposiciones y examinar periódicamente su aplicación; c) ha establecido procedimientos y estructuras para tratar las reclamaciones relativas a infracciones del código o a la manera en que el código haya sido o esté siendo aplicado por un responsable o encargado del tratamiento, y para hacer dichos procedimientos y estructuras transparentes para los interesados y el público, y d) ha demostrado, a satisfacción de la autoridad de control competente, que sus funciones y cometidos no dan lugar a conflicto de intereses. 3. La autoridad de control competente someterá al Comité, con arreglo al mecanismo de coherencia a que se refiere el artículo 63, el proyecto que fije los criterios de acreditación de un organismo a que se refiere el apartado 1 del presente artículo. 4. Sin perjuicio de las funciones y los poderes de la autoridad de control competente y de lo dispuesto en el capítulo VIII, un organismo a tenor del apartado 1 del presente artículo deberá, con sujeción a garantías adecuadas, tomar las medidas oportunas en caso de infracción del código por un responsable o encargado del tratamiento, incluida la suspensión o exclusión de este. Informará de dichas medidas y de las razones de estas a la autoridad de control competente. 5. La autoridad de control competente revocará la acreditación de un organismo a tenor del apartado 1 si las condiciones de la acreditación no se cumplen o han dejado de cumplirse, o si la actuación de dicho organismo infringe el presente Reglamento. 6. El presente artículo no se aplicará al tratamiento realizado por autoridades y organismos públicos".

Artículo 43 del RGPD; "Organismo de certificación 1. Sin perjuicio de las funciones y poderes de la autoridad de control competente en virtud de los artículos 57 y 58, los organismos de certificación que tengan un nivel adecuado de pericia en materia de protección de datos expedirán y renovarán las certificaciones una vez informadas la autoridad de control, a fin de esta que pueda ejercer, si así se requiere, sus poderes en virtud del artículo 58, apartado 2, letra h). Los Estados miembros garantizarán que dichos organismos de certificación sean acreditados por la autoridad o el organismo indicado a continuación, o por ambos: a) la autoridad de control que sea competente en virtud del artículo 55 o 56; b) el organismo nacional de acreditación designado de conformidad con el Reglamento (CE) n.o 765/2008 del Parlamento Europeo y del Consejo con arreglo a la norma EN ISO/IEC 17065/2012 y a los requisitos adicionales establecidos por la autoridad de control que sea competente en virtud del artículo 55 o 56. 2. Los organismos de certificación mencionados en el apartado 1 únicamente serán acreditados de conformidad con dicho apartado si: a) han demostrado, a satisfacción de la autoridad de control competente, su independencia y su pericia en relación con el objeto de la certificación; b) se han comprometido a respetar los criterios mencionados en el artículo 42, apartado 5, y aprobados por la autoridad de control que sea competente en virtud del artículo 55 o 56, o por el Comité de conformidad con el artículo 63; c) han establecido procedimientos para la expedición, la revisión periódica y la retirada de certificaciones, sellos y marcas de protección de datos; d) han establecido procedimientos y estructuras para tratar las reclamaciones relativas a infracciones de la certificación o a la manera en que la certificación haya

sido o esté siendo aplicada por un responsable o encargado del tratamiento, y para hacer dichos procedimientos y estructuras transparentes para los interesados y el público, y e) han demostrado, a satisfacción de la autoridad de control competente, que sus funciones y cometidos no dan lugar a conflicto de intereses. 3. La acreditación de los organismos de certificación a que se refieren los apartados 1 y 2 del presente artículo se realizará sobre la base de los criterios aprobados por la autoridad de control que sea competente en virtud del artículo 55 o 56, o por el Comité de conformidad con el artículo 63. En caso de acreditación de conformidad con el apartado 1, letra b), del presente artículo, estos requisitos complementarán los contemplados en el Reglamento (CE) n.o 765/2008 y las normas técnicas que describen los métodos y procedimientos de los organismos de certificación. 4. Los organismos de certificación a que se refiere el apartado 1 serán responsable de la correcta evaluación a efectos de certificación o retirada de la certificación, sin perjuicio de la responsabilidad del responsable o del encargado del tratamiento en cuanto al cumplimiento del presente Reglamento. La acreditación se expedirá por un período máximo de cinco años y podrá ser renovada en las mismas condiciones, siempre y cuando el organismo de certificación cumpla los requisitos establecidos en el presente artículo. 5. Los organismos de certificación a que se refiere el apartado 1 comunicarán a las autoridades de control competentes las razones de la expedición de la certificación solicitada o de su retirada. 6. La autoridad de control hará públicos los requisitos a que se refiere el apartado 3 del presente artículo y los criterios a que se ha refiere el artículo 42, apartado 5, en una forma fácilmente accesible. Las autoridades de control comunicarán también dichos requisitos y criterios al Comité. El Comité archivará en un registro todos los mecanismos de certificación y sellos de protección de datos y los pondrá a disposición pública por cualquier medio apropiado. 7. No obstante lo dispuesto en el capítulo VIII, la autoridad de control competente o el organismo nacional de acreditación revocará la acreditación a un organismo de certificación a tenor del apartado 1 del presente artículo si las condiciones de la acreditación no se cumplen o han dejado de cumplirse, o si la actuación de dicho organismo de certificación infringe el presente Reglamento. 8. La Comisión estará facultada para adoptar actos delegados, de conformidad con el artículo 92, a fin de especificar las condiciones que deberán tenerse en cuenta para los mecanismos de certificación en materia de protección de datos a que se refiere el artículo 42, apartado 1. 9. La Comisión podrá adoptar actos de ejecución que establezcan normas técnicas para los mecanismos de certificación y los sellos y marcas de protección de datos, y mecanismos para promover y reconocer dichos mecanismos de certificación, sellos y marcas. Dichos actos de ejecución se adoptarán con arreglo al procedimiento de examen a que se refiere el artículo 93, apartado 2".

Dentro de la función de promoción también es posible distinguir las facilidades que la autoridad de control entregue a los responsables y encargados del tratamiento de datos mediante la adopción de cláusulas contractuales tipo con las garantías adecuadas.

Asimismo, la función de promoción de la autoridad de control dirigida hacia los ciudadanos se expresa en sensibilizar al público para que comprendan los riesgos, normas, garantías y derechos relacionados con el tratamiento de datos de carácter personal, incluyendo con especial atención aquellas actividades de sensibilización dirigidas a los niños. Además de previa solicitud, facilitar información a cualquier interesado en relación con el ejercicio de sus

derechos y, en su caso, cooperar a tal fin con las autoridades de control de otros Estados miembros y hacer un seguimiento de cambios que sean de interés, en la medida en que tengan incidencia en la protección de datos personales, en particular el desarrollo de las tecnologías de la información y la comunicación y las prácticas comerciales.

c) La Función de Cooperación

El Reglamento les impone a las autoridades de control el deber de establecer criterios comunes relacionados con la vigencia de la protección de datos personales como derecho fundamental. Debiendo cooperar, en particular compartiendo información, con otras autoridades de control y prestar asistencia mutua con el fin de garantizar la coherencia en la aplicación y ejecución del Reglamento, contribuyendo con ello a las actividades que realice el Comité Europeo de Protección de Datos.

La función de cooperación se plasma también en el considerando 123 del Reglamento del cual se desprende que:

> *"A fin de proteger a las personas físicas con respecto al tratamiento de sus datos personales y de facilitar la libre circulación de los datos personales en el mercado interior, las autoridades de control deben supervisar la aplicación de las disposiciones adoptadas de conformidad con el presente Reglamento y contribuir a su aplicación coherente en toda la Unión. A tal efecto, las autoridades de control deben cooperar entre ellas y con la Comisión, sin necesidad de acuerdo alguno entre Estados miembros sobre la prestación de asistencia mutua ni sobre dicha cooperación".*

Incluso el considerando 116 del RGPD destaca esta función de cooperación, más allá de las fronteras de los Estados miembros de la Unión, al señalar:

> *"Cuando los datos personales circulan a través de las fronteras hacia el exterior de la Unión se puede poner en mayor riesgo la capacidad de las personas físicas para ejercer los derechos de protección de datos, en particular con el fin de protegerse contra la utilización o comunicación ilícitas de dicha información. Al mismo tiempo, es posible que las autoridades de control se vean en la imposibilidad de tramitar reclamaciones o realizar investigaciones relativas a actividades desarrolladas fuera de sus fronteras. Sus esfuerzos por colaborar en el contexto transfronterizo también pueden verse obstaculizados por poderes preventivos o correctivos insuficientes, regímenes jurídicos incoherentes y obstáculos prácticos, como la escasez de recursos. Por consiguiente, es necesario fomentar una cooperación más estrecha entre las autoridades de control encargadas de la protección de datos para ayudarlas a intercambiar información y a llevar a cabo investigaciones con sus homólogos internacionales. A fin de desarrollar mecanismos de cooperación internacional que faciliten y proporcionen asistencia internacional mutua en la ejecución de legislación en materia de protección de datos personales, la Comisión y las autoridades de control deben intercambiar información y cooperar en actividades relativas al ejercicio de sus competencias con las autoridades competentes de terceros países, sobre la base de la reciprocidad y de conformidad con el presente Reglamento".*

Finalmente, en relación con las funciones de promoción y principalmente de prestación que desarrollan las autoridades de control para la protección en el tratamiento de datos de carácter

personal, es importante señalar que según se desprende del artículo 57 apartado 3 del RGPD el desempeño de las funciones de cada autoridad de control será gratuito para el interesado y, en su caso, para el delegado de protección de datos. Igualmente, cuando los requerimientos o solicitudes ante la autoridad de control sean manifiestamente infundados o excesivos, especialmente debido a su carácter repetitivo, la autoridad de control podrá establecer una tasa razonable basada en los costes administrativos o negarse a actuar respecto de la solicitud. La carga de demostrar el carácter manifiestamente infundado o excesivo de la solicitud recaerá en la autoridad de control.

Poderes

Los poderes de la autoridad de control están establecidos en el artículo 58 del Reglamento y constituyen los instrumentos jurídicos que le permiten a esta hacer cumplir las disposiciones contenidas en dicha normativa general y obligatoria para todos los Estados miembros de la Unión. Estos poderes le otorgan carácter ejecutivo a las decisiones que adopte la autoridad de control, la que no solo crea o dicta disposiciones, si no que en virtud de estos poderes puede directamente exigir el cumplimiento de los actos que dicta o realiza, siendo dichos actos vinculantes para sus destinatarios.

A la forma, contenido, alcance y ejercicio de estos poderes se refiere el considerando 129 del Reglamento, del cual es posible extraer lo siguiente:

Para garantizar la supervisión y ejecución coherentes del presente Reglamento en toda la Unión, las autoridades de control deben tener en todos los Estados miembros las mismas funciones y poderes efectivos, incluidos poderes de investigación, poderes correctivos y sancionadores, y poderes de autorización y consultivos, especialmente en casos de reclamaciones de personas físicas, y sin perjuicio de las competencias de las autoridades encargadas de la persecución de los delitos con arreglo al Derecho de los Estados miembros para poner en conocimiento de las autoridades judiciales las infracciones del Reglamento y ejercitar acciones judiciales.

Es decir, el RGPD busca uniformar en todos los Estados miembros las funciones y poderes de las autoridades de control, para asegurar su coherencia y cumplimiento, facilitando cuando corresponda a los órganos jurisdiccionales respectivos, los antecedentes derivados de las infracciones a sus disposiciones.

El Reglamento distingue también tres tipos de poderes: los poderes de investigación, poderes correctivos y poderes de autorización y consultivos. Dichos poderes deben incluir además el poder de imponer una limitación temporal o definitiva al tratamiento, incluida su prohibición.

Los poderes de las autoridades de control deben ejercerse de conformidad con garantías procesales adecuadas establecidas en el Derecho de la Unión y los Estados miembros, de forma imparcial, equitativa y en un plazo razonable. En particular, toda medida debe ser adecuada, necesaria y proporcionada con vistas a garantizar el cumplimiento del presente Reglamento, teniendo en cuenta las circunstancias de cada caso concreto, respetar el derecho de todas las personas a ser oídas antes de que se adopte cualquier medida que las afecte negativamente y evitar costes superfluos y molestias excesivas para las personas afectadas.

Es decir, el RGPD refuerza los principios del debido proceso en el ejercicio de los poderes de las autoridades de control, así como la bilateralidad de la audiencia y la proporcionalidad en las medidas adoptadas.

Los poderes de investigación, en lo que se refiere al acceso a instalaciones, deben ejercerse de conformidad con los requisitos específicos del derecho procesal de los Estados miembros, como el de la autorización judicial previa. Toda medida jurídicamente vinculante de la autoridad de control debe constar por escrito, ser clara e inequívoca, indicar la autoridad de control que dictó la medida y la fecha en que se dictó, llevar la firma del director o de un miembro de la autoridad de control autorizado por este, especificar los motivos de la medida y mencionar el derecho a la tutela judicial efectiva.

Por consiguiente, las medidas vinculantes que la autoridad de control adopte, deben expresarse formalmente y de manera explícita e inequívoca, singularizarse y suscribirse por quien la expidió y contener los sustentos jurídicos y facticos que la justifican.

Lo anterior no obsta a que se impongan requisitos adicionales con arreglo al derecho procesal de los Estados miembros. La adopción de una decisión jurídicamente vinculante implica que puede ser objeto de control judicial en el Estado miembro de la autoridad de control que adoptó la decisión, siguiendo entonces la regla de impugnabilidad de las actuaciones de los órganos de la administración.

A. Los Poderes de Investigación

Están descritos en el apartado 1 del artículo 58 del Reglamento, el cual señala que;

"Cada autoridad de control dispondrá de todos los poderes de investigación indicados a continuación:

a) ordenar al responsable y al encargado del tratamiento y, en su caso, al representante del responsable o del encargado, que faciliten cualquier información que requiera para el desempeño de sus funciones;

b) llevar a cabo investigaciones en forma de auditorías de protección de datos;

c) llevar a cabo una revisión de las certificaciones expedidas en virtud del artículo 42, apartado 7;

d) notificar al responsable o al encargado del tratamiento las presuntas infracciones del presente Reglamento;

e) obtener del responsable y del encargado del tratamiento el acceso a todos los datos personales y a toda la información necesaria para el ejercicio de sus funciones;

f) obtener el acceso a todos los locales del responsable y del encargado del tratamiento, incluidos cualesquiera equipos y medios de tratamiento de datos, de conformidad con el Derecho procesal de la Unión o de los Estados miembros".

B. Los Poderes Correctivos

Están consagrados en el apartado dos del artículo 58, el cual establece que Cada autoridad de control dispondrá de todos los siguientes poderes correctivos indicados a continuación:

a) sancionar a todo responsable o encargado del tratamiento con una advertencia cuando las operaciones de tratamiento previstas puedan infringir lo dispuesto en el presente Reglamento;
b) sancionar a todo responsable o encargado del tratamiento con apercibimiento cuando las operaciones de tratamiento hayan infringido lo dispuesto en el presente Reglamento;
c) ordenar al responsable o encargado del tratamiento que atiendan las solicitudes de ejercicio de los derechos del interesado en virtud del presente Reglamento;
d) ordenar al responsable o encargado del tratamiento que las operaciones de tratamiento se ajusten a las disposiciones del presente Reglamento, cuando proceda, de una determinada manera y dentro de un plazo especificado;
e) ordenar al responsable del tratamiento que comunique al interesado las violaciones de la seguridad de los datos personales;
f) imponer una limitación temporal o definitiva del tratamiento, incluida su prohibición;
g) ordenar la rectificación o supresión de datos personales o la limitación de tratamiento con arreglo a los artículos 16, 17 y 18 y la notificación de dichas medidas a los destinatarios a quienes se hayan comunicado datos personales con arreglo a al artículo 17, apartado 2, y al artículo 19;
h) retirar una certificación u ordenar al organismo de certificación que retire una certificación emitida con arreglo a los artículos 42 y 43, u ordenar al organismo de certificación que no se emita una certificación si no se cumplen o dejan de cumplirse los requisitos para la certificación;
i) imponer una multa administrativa con arreglo al artículo 83, además o en lugar de las medidas mencionadas en el presente apartado, según las circunstancias de cada caso particular;
j) ordenar la suspensión de los flujos de datos hacia un destinatario situado en un tercer país o hacia una organización internacional.

C. Poderes de Autorización y Consultivos

Finalmente, el apartado 3 del artículo 58 se refiere a los poderes de autorización y consultivos, señalando que cada autoridad de control dispondrá de todos los poderes de autorización y consultivos indicados a continuación:

a) asesorar al responsable del tratamiento conforme al procedimiento de consulta previa contemplado en el artículo 36;
b) emitir, por iniciativa propia o previa solicitud, dictámenes destinados al Parlamento nacional, al Gobierno del Estado miembro o, con arreglo al Derecho de los Estados miembros, a otras instituciones y organismos, así como al público, sobre cualquier asunto relacionado con la protección de los datos personales;
c) autorizar el tratamiento a que se refiere el artículo 36, apartado 5, si el Derecho del Estado miembro requiere tal autorización previa;

d) emitir un dictamen y aprobar proyectos de códigos de conducta de conformidad con lo dispuesto en el artículo 40, apartado 5;
e) acreditar los organismos de certificación con arreglo al artículo 43;
f) expedir certificaciones y aprobar criterios de certificación con arreglo al artículo 42, apartado 5;
g) adoptar las cláusulas tipo de protección de datos contempladas en el artículo 28, apartado 8, y el artículo 46, apartado 2, letra d);
h) autorizar las cláusulas contractuales indicadas en el artículo 46, apartado 3, letra a);
i) autorizar los acuerdos administrativos contemplados en el artículo 46, apartado 3, letra b);
j) aprobar normas corporativas vinculantes de conformidad con lo dispuesto en el artículo 47.

Por último, el artículo 59 del Reglamento se refiere a que cada autoridad de control elaborará un informe anual de sus actividades, que podrá incluir una lista de tipos de infracciones notificadas y de tipos de medidas adoptadas de conformidad con el artículo 58, apartado 2. Los informes se transmitirán al Parlamento Nacional, al Gobierno y a las demás autoridades designadas en virtud del Derecho de los Estados miembros. Se pondrán a disposición del público, de la Comisión y del Comité Europeo de Protección de Datos.

El Tratamiento Internacional y Transfronterizo de datos Personales y la Autoridad de Control

El RGPD, antes de referirse a la Autoridad de Control, regula en el Capítulo V, entre los artículos 44 y 50, la Transferencias de datos personales a terceros países u organizaciones internacionales, sin embargo, no conceptualiza qué se entiende por transferencia internacional de datos, abordando solo lo relativo al tratamiento transfronterizo. En efecto, el artículo 4 del RGPD en su numeral 23 se refiere al "tratamiento transfronterizo", como: "el tratamiento de datos personales realizado en el contexto de las actividades de establecimientos en más de un Estado miembro de un responsable o un encargado del tratamiento en la Unión, si el responsable o el encargado está establecido en más de un Estado miembro, o el tratamiento de datos personales realizado en el contexto de las actividades de un único establecimiento de un responsable o un encargado del tratamiento en la Unión, pero que afecta sustancialmente o es probable que afecte sustancialmente a interesados en más de un Estado miembro".

El Principio general para la transferencia de datos se encuentra contenido en el artículo 44 del RGPD, el cual dispone:

"*Solo se realizarán transferencias de datos personales que sean objeto de tratamiento o vayan a serlo tras su transferencia a un tercer país u organización internacional si, a reserva de las demás disposiciones del presente Reglamento, el responsable y el encargado del tratamiento cumplen las condiciones establecidas en el presente capítulo, incluidas las relativas a las transferencias ulteriores de datos personales desde el tercer país u organización internacional a otro tercer país u otra organización internacional. Todas las disposiciones del presente capítulo se aplicarán a fin de asegurar que el nivel de protección de las personas físicas garantizado por el presente Reglamento no se vea menoscabado*".

En lo sustancial somete toda transferencia de datos a la sujeción de las normas contenidas en el Reglamento de la UE.

Como se ha señalado el RGPD no define la transferencia internacional de datos, cuestión que tampoco era regulada por la Directiva 95/46/CE. Concepto que sí estaba señalado en la antigua normativa española y que tampoco recoge la actual Ley Orgánica 3/2018.

En efecto, el Reglamento español de Protección de Datos, en el artículo 5.1 s) explicaba la Transferencia internacional de datos como: *"Tratamiento de datos que supone una transmisión de los mismos fuera del territorio del Espacio Económico Europeo, bien constituya una cesión o comunicación de datos, bien tenga por objeto la realización de un tratamiento de datos por cuenta del responsable del fichero establecido en territorio español"*.

Autores como Álvarez Rigaudias definen la transferencia de datos personales como "la transmisión directa de datos a consecuencia de la cual el transmitente da acceso o permite el conocimiento de ellos al destinatario (distinto del afectado), implicando por tanto una comunicación material de datos personales con independencia de su finalidad (sin perjuicio de las implicaciones legales especificas previstas para las comunicaciones de datos a terceros para realizar tratamientos por cuenta del transmitente o para otras finalidades); siendo internacional cuando el destino de los datos (o desde donde se accede a los datos) se localiza fuera de la UE/EEE (Espacio Económico Europeo)[513]".

Así entonces, la diferencia entre la transferencia internacional de datos y el tratamiento transfronterizo de datos está en que la primera involucra a países u organizaciones internacionales[514] que están fuera de la UE, y la segunda, esto es, el tratamiento transfronterizo, involucra las operaciones o tratamiento de datos al interior de las fronteras de la propia UE.

Como señala Berrocal Lanzarot,[515] el tratamiento internacional alcanza al tratamiento de datos que se transfieren fuera del Espacio Económico Europeo (EEE), que incluye además de los Estados miembros de la Unión Europea a Islandia, Liechtenstein y Noruega; y el tratamiento transfronterizo considera el tratamiento de datos realizado en el contexto de actividades de los diferentes establecimientos del responsable o encargado del tratamiento situado en más de un Estado miembro, o en un único establecimiento, pero que afecte a interesados en más de un Estado miembro. Esta transferencia de datos solo tiene operatividad en el seno de la propia Unión Europea, pues no traspasa las fronteras de la Unión, ni tampoco afecta a interesados extracomunitarios.

---

[513] Álvarez Rigaudias C. (2018), "Transferencias de datos personales a terceros países y organizaciones internacionales (artículos 44-50)", en "*El nuevo marco regulatorio de derivado del Reglamento Europeo de Protección de Datos. Adaptado al proyecto de Ley Orgánica de Protección de Datos de 10 de noviembre de 2017"*, coordinador José López Calvo, Boch, Barcelona, pp.563-564; de la misma autora, "Transferencia de Datos Personales a terceros países y organizaciones internacionales (Artículos 44-50 del RGPD. Artículos 40-43 y disposición adicional quinta y decimotercera de la LOPDGDD)", "*La adaptación al nuevo marco de protección de datos tras el RGPD y la LOPDGDD"*, coordinador José López Calvo, Boch, Barcelona 2019, p.570.

[514] El artículo 4 numeral 26 del RGPD define organización internacional como "una organización internacional y sus entes subordinados de Derecho Internacional público o cualquier otro organismo creado mediante un acuerdo entre dos o más países o en virtud de tal acuerdo".

[515] Berrocal Lanzarot, A. (2019), "Estudio Jurídico-Crítico sobre la Ley Orgánica 2/2018, de 5 de Diciembre de Protección de Datos Personales y Garantías de Derechos Digitales", Reus, Madrid, p. 549.

De lo expuesto, resulta fundamental para el desarrollo de la investigación que aquí se expone, referirse a los supuestos en virtud de los cuales se puede realizar una transferencia internacional de datos a países u organismos internacionales que se sitúan fuera de la UE, en el entendido que siempre debe resguardarse la protección de datos de cualquier individuo o persona física por parte del responsable y encargado del tratamiento, sujetándose a las normas del RGPD, las que se encuentran contenidas principalmente en los artículos 45, 46 y 49. Disposiciones que se refieren a las transferencias basadas en criterios de adecuación, garantías adecuadas y excepciones para situaciones específicas, respectivamente[516].

Transferencias Basadas en un Nivel de Protección Adecuado (artículo 45 del RGPD)

El apartado número 1 del artículo 45 dispone que:

> *"Podrá realizarse una transferencia de datos personales a un tercer país u organización internacional cuando la Comisión haya decidido que el tercer país, un territorio o uno o varios sectores específicos de ese tercer país, o la organización internacional de que se trate garantizan un nivel de protección adecuado. Dicha transferencia no requerirá ninguna autorización específica"*.

Por lo expuesto, la normativa europea, entonces, coloca el énfasis en el "nivel de protección adecuado" que no está definido, constituyendo por consiguiente un concepto jurídico indeterminado, sin embargo, el considerando 104 del propio Reglamento ofrece algunas orientaciones sobre la materia, al señalar "… En la adopción de una decisión de adecuación con respecto a un territorio o un sector específico de un tercer país se deben tener en cuenta criterios claros y objetivos, como las actividades concretas de tratamiento y el alcance de las normas jurídicas aplicables y la legislación vigente en el tercer país. El tercer país debe ofrecer garantías que aseguren un nivel adecuado de protección equivalente, en lo esencial, al ofrecido en la Unión, en particular cuando los datos personales son objeto de tratamiento en uno o varios sectores específicos. En particular, el tercer país debe garantizar que haya un control verdaderamente independiente de la protección de datos y establecer mecanismos de cooperación con las autoridades de protección de datos de los Estados miembros, así como reconocer a los interesados derechos efectivos y exigibles y acciones administrativas y judiciales efectivas".

Al igual que lo señala el artículo 45.1 del RGPD, quien determina o pondera que ese tercer país u organismo internacional garantiza un nivel adecuado de protección es la Comisión de la UE, lo que es refrendado por el considerando 103 del propio Reglamento que señala

> *"La Comisión puede decidir, con efectos para toda la Unión, que un tercer país, un territorio o un sector específico de un tercer país, o una organización internacional ofrece un nivel de protección de datos adecuado, aportando de esta forma en toda la Unión seguridad y uniformidad jurídicas en lo que se refiere al tercer país u*

[516]En el caso español, la LPDPGDD 3/2018, en su Artículo 40 dispone sobre el Régimen de las transferencias internacionales de datos que: "Las transferencias internacionales de datos se regirán por lo dispuesto en el Reglamento (UE) 2016/679, en la presente ley orgánica y sus normas de desarrollo aprobadas por el Gobierno, y en las circulares de la Agencia Española de Protección de Datos y de las autoridades autonómicas de protección de datos, en el ámbito de sus respectivas competencias. En todo caso se aplicarán a los tratamientos en que consista la propia transferencia las disposiciones contenidas en dichas normas, en particular las que regulan los principios de protección de datos".

organización internacional que se considera ofrece tal nivel de protección. En estos casos, se pueden realizar transferencias de datos personales a estos países sin que se requiera obtener otro tipo de autorización. La Comisión también puede decidir revocar esa decisión, previo aviso y completa declaración motivada al tercer país u organización internacional".

Para realizar esta ponderación el RGPD en el artículo 45.2 se refiere a los elementos que deberá tener en consideración la Comisión, los cuales son:

a) El Estado de Derecho, el respeto de los derechos humanos y las libertades fundamentales, la legislación pertinente, tanto general como sectorial, incluida la relativa a la seguridad pública, la defensa, la seguridad nacional y la legislación penal, y el acceso de las autoridades públicas a los datos personales, así como la aplicación de dicha legislación, las normas de protección de datos, las normas profesionales y las medidas de seguridad, incluidas las normas sobre transferencias ulteriores de datos personales a otro tercer país u organización internacional observadas en ese país u organización internacional, la jurisprudencia, así como el reconocimiento a los interesados cuyos datos personales estén siendo transferidos de derechos efectivos y exigibles y de recursos administrativos y acciones judiciales que sean efectivos;

b) La existencia y el funcionamiento efectivo de una o varias autoridades de control independientes en el tercer país o a las cuales esté sujeta una organización internacional, con la responsabilidad de garantizar y hacer cumplir las normas en materia de protección de datos, incluidos poderes de ejecución adecuados, de asistir y asesorar a los interesados en el ejercicio de sus derechos, y de cooperar con las autoridades de control de la Unión y de los Estados miembros[517].

c) Los compromisos internacionales asumidos por el tercer país u organización internacional de que se trate, u otras obligaciones derivadas de acuerdos o instrumentos jurídicamente vinculantes, así como de su participación en sistemas multilaterales o regionales, en particular en relación con la protección de los datos personales.

El considerando 105 del RGPD complementa lo indicando en el Artículo 45.2 sobre los instrumentos jurídicos internacionales al disponer que:

"Aparte de los compromisos internacionales adquiridos por el tercer país u organización internacional, la Comisión debe tener en cuenta las obligaciones resultantes de la participación del tercer país u organización internacional en sistemas multilaterales o regionales, en particular en relación con la protección de los datos personales, y el cumplimiento de esas obligaciones. En particular, debe tenerse en cuenta la adhesión del país al Convenio del Consejo de Europa, de 28 de enero de 1981, para la protección de las personas con respecto al tratamiento automatizado de

[517] Como se puede observar, el establecimiento de una Autoridad de Control independiente es un elemento sustancial para determinar que un país tiene un nivel adecuado de protección de datos, autoridad que debe tener las competencias y funciones que le permitan regular, promover y tutelar el tratamiento de datos de las personas físicas.

> *datos de carácter personal y su Protocolo adicional. La Comisión debe consultar al Comité al evaluar el nivel de protección existente en terceros países u organizaciones internacionales"*.

Los numerales 3 al 9 del artículo 45 del RGPD se refieren al procedimiento a seguir por la Comisión para ponderar el adecuado nivel de protección de datos; en lo sustancial, de estas disposiciones se desprende que la Comisión, tras haber evaluado la adecuación del nivel de protección, podrá decidir, mediante un acto de ejecución, que un tercer país, un territorio o uno o varios sectores específicos de un tercer país, o una organización internacional garantizan un nivel de protección adecuado según los elementos ya indicados. El acto de ejecución establecerá un mecanismo de revisión periódica, al menos cada cuatro años, que tenga en cuenta todos los acontecimientos relevantes en el tercer país o en la organización internacional. El acto de ejecución especificará su ámbito de aplicación territorial y sectorial, y, en su caso, determinará la autoridad o autoridades de control.

Además, la Comisión publicará en el Diario Oficial de la Unión Europea y en su página web una lista de terceros países, territorios y sectores específicos en un tercer país, y organizaciones internacionales respecto de los cuales haya decidido que se garantiza, o ya no, un nivel de protección adecuado.

La regulación que determina el nivel adecuado para el tratamiento de datos a países fuera de la UE es mucho más riguroso que el establecido bajo el imperio de la Directiva 95/46/CE, en efecto el Grupo del artículo 29 sobre Protección de Datos intentó identificar el nivel de cumplimiento y la disponibilidad de mecanismos para tal efecto, tales como recursos judiciales y sistema de sanciones. El elemento distintivo de la Directiva 95/46/CE en este punto fue la existencia de una autoridad independiente que supervisara el cumplimento de la ley; de hecho, este elemento ha sido consagrado como una parte esencial del derecho a la protección de los datos personales previsto en la Carta de los Derechos Fundamentales de la Unión Europea. Sin embargo, el Grupo del artículo 29 sobre Protección de Datos no se concentró en un determinado mecanismo sino que miro hacia los propósitos subyacentes del sistema: la obtención de un buen nivel de cumplimiento de las normas, el apoyo y ayuda hacia los titulares de datos personales para el ejercicio de sus derechos, y la provisión de apropiadas compensaciones para las partes afectadas con la infracción de las reglas. En suma, como es posible apreciar, el Grupo del artículo 29 sobre Protección de Datos adoptó criterios más flexibles a efectos de establecer si un determinado país provee un "nivel adecuado de protección" y, consecuentemente, podía disfrutar de transferencias de datos personales desde los países miembros de la Unión Europea. Sobre la base de un análisis caso a caso, estos criterios intentan identificar si un país garantiza adecuada protección, a través de la adopción y el cumplimiento de las normas relativas a la protección de los datos personales[518].

Transferencias mediante garantías adecuadas (artículo 46 del RGPD)

En ausencia de una decisión por la que se constate la adecuada protección de los datos, el responsable o el encargado del tratamiento deben tomar medidas para compensar la falta de

[518] Cerda Silva, Alberto. (2011). El "nivel adecuado de protección" para las transferencias internacionales de datos personales desde la Unión Europea. *Revista de derecho (Valparaíso)*, (36), 327-356. https://dx.doi.org/10.4067/S0718-68512011000100009

protección de datos en un tercer país mediante garantías para el interesado. Tales garantías pueden consistir en a normas corporativas vinculantes, a cláusulas tipo de protección de datos adoptadas por la Comisión o por una autoridad de control, o a cláusulas contractuales autorizadas por una autoridad de control. Esas garantías deben asegurar la observancia de requisitos de protección de datos y derechos de los interesados adecuados al tratamiento dentro de la Unión, incluida la disponibilidad por parte de los interesados de derechos exigibles y de acciones legales efectivas, lo que incluye el derecho a obtener una reparación administrativa o judicial efectiva y a reclamar una indemnización, en la Unión o en un tercer país. En particular, deben referirse al cumplimiento de los principios generales relativos al tratamiento de los datos personales y los principios de la protección de datos desde el diseño y por defecto.

Las transferencias también pueden realizarlas autoridades o entidades públicas con entidades o autoridades públicas de terceros países o con organizaciones internacionales con competencias o funciones correspondientes, igualmente sobre la base de disposiciones incorporadas en acuerdos administrativos, como un memorando de entendimiento, que reconozcan derechos exigibles y efectivos a los interesados. Si las garantías figuran en acuerdos administrativos que no sean jurídicamente vinculantes se debe recabar la autorización de la autoridad de control competente[519].

En cualquier caso, cuando la Comisión no haya tomado ninguna decisión sobre el nivel adecuado de la protección de datos en un tercer país, el responsable o el encargado del tratamiento deben arbitrar soluciones que garanticen a los interesados derechos exigibles y efectivos con respecto al tratamiento de sus datos en la Unión, una vez transferidos estos, de forma que sigan beneficiándose de derechos fundamentales y garantías[520].

Así entonces, si no existe una decisión por la que se determine la adecuación de la protección de datos, el responsable o el encargado del tratamiento solo podrá transferir datos personales a un 3° país u organización internacional si ofrece garantías adecuadas, las que pueden formalizarse a través de una serie de instrumentos que pueden requerir o no autorización expresa de una autoridad de control. Entre los instrumentos que no requieren autorización expresa de la autoridad de control el artículo 46.2 del RGPD distingue: a) un instrumento jurídicamente vinculante y exigible entre las autoridades u organismos públicos; b) normas corporativas vinculantes[521] de conformidad con el artículo 47; c) cláusulas tipo de protección de datos adoptadas por la Comisión de conformidad con el procedimiento de examen a que se refiere el artículo 93, apartado 2; d) cláusulas tipo de protección de datos adoptadas por una autoridad de control y aprobadas por la Comisión con arreglo al procedimiento de examen a que se refiere en el artículo 93, apartado 2; e) un código de conducta aprobado con arreglo al artículo 40, junto con compromisos vinculantes y exigibles del responsable o el encargado del tratamiento en el tercer país de aplicar garantías adecuadas, incluidas la relativas a los derechos de los interesados, o f) un mecanismo de certificación aprobado con arreglo al artículo 42,

[519] Considerando 108 del RGPD.

[520] Considerando 114 del RGPD.

[521] Las “normas corporativas vinculantes”, están definidas en el artículo 4. 20 del RGPD como “las políticas de protección de datos personales asumidas por un responsable o encargado del tratamiento establecido en el territorio de un Estado miembro para transferencias o un conjunto de transferencias de datos personales a un responsable o encargado en uno o más países terceros, dentro de un grupo empresarial o una unión de empresas dedicadas a una actividad económica conjunta”.

junto con compromisos vinculantes y exigibles del responsable o el encargado del tratamiento en el tercer país de aplicar garantías adecuadas, incluidas la relativas a los derechos de los interesados.

También el artículo 46.3 se refiere a aquellos instrumentos en que existiendo autorización de la autoridad de control competente, las garantías contempladas en el apartado 1 del mismo artículo 46 podrán igualmente ser aportadas mediante dos mecanismos: a) cláusulas contractuales entre el responsable o el encargado y el responsable, encargado o destinatario de los datos personales en el tercer país u organización internacional, o b) disposiciones que se incorporen en acuerdos administrativos entre las autoridades u organismos públicos que incluyan derechos efectivos y exigibles para los interesados. Para ello, la Autoridad de Control competente aplicará el mecanismo de coherencia a que se refiere el artículo 63 del RGPD[522].

Transferencias con Excepciones para situaciones específicas

El artículo 49 del RGPD establece en su apartado N° 1, que:

> *"En ausencia de una decisión de adecuación de conformidad con el artículo 45, apartado 3, o de garantías adecuadas de conformidad con el artículo 46, incluidas las normas corporativas vinculantes, una transferencia o un conjunto de transferencias de datos personales a un tercer país u organización internacional únicamente se realizará si se cumple alguna de las condiciones siguientes: a) el interesado haya dado explícitamente su consentimiento a la transferencia propuesta, tras haber sido informado de los posibles riesgos para él de dichas transferencias debido a la ausencia de una decisión de adecuación y de garantías adecuadas; b) la transferencia sea necesaria para la ejecución de un contrato entre el interesado y el responsable del tratamiento o para la ejecución de medidas precontractuales adoptadas a solicitud del interesado; c) la transferencia sea necesaria para la celebración o ejecución de un contrato, en interés del interesado, entre el responsable del tratamiento y otra persona física o jurídica; d) la transferencia sea necesaria por razones importantes de interés público; e) la transferencia sea necesaria para la formulación, el ejercicio o la defensa de reclamaciones; f) la transferencia sea necesaria para proteger los intereses vitales del interesado o de otras personas, cuando el interesado esté física o jurídicamente incapacitado para dar su consentimiento; g) la transferencia se realice desde un registro público que, con arreglo al Derecho de la Unión o de los Estados miembros, tenga por objeto facilitar información al público y esté abierto a la consulta del público en general o de cualquier persona que pueda acreditar un interés legítimo, pero sólo en la medida en que se cumplan, en cada caso particular, las condiciones que establece el Derecho de la Unión o de los Estados miembros para la consulta".*

Si bien una transferencia efectuada de conformidad con la letra g) precedente, no abarcará la totalidad de los datos personales ni categorías enteras de datos personales contenidos en el registro. Si la finalidad del registro es la consulta por parte de personas que tengan un interés

[522] El Artículo 63 del RGPD, dispone "A fin de contribuir a la aplicación coherente del presente Reglamento en toda la Unión, las autoridades de control cooperarán entre sí y, en su caso, con la Comisión, en el marco del mecanismo de coherencia establecido en la presente sección".

legítimo, la transferencia solo se efectuará a solicitud de dichas personas o si estas han de ser las destinatarias.

Cuando una transferencia no pueda basarse en las disposiciones de los artículos 45 o 46, incluidas las disposiciones sobre normas corporativas vinculantes, y no sea aplicable ninguna de las excepciones para situaciones específicas a que se refiere el párrafo primero del presente apartado, solo se podrá llevar a cabo si no es repetitiva, afecta solo a un número limitado de interesados, es necesaria a los fines de intereses legítimos imperiosos perseguidos por el responsable del tratamiento sobre los que no prevalezcan los intereses o derechos y libertades del interesado, y el responsable del tratamiento evaluó todas las circunstancias concurrentes en la transferencia de datos y, basándose en esta evaluación, ofreció garantías apropiadas con respecto a la protección de datos personales.

Lo expuesto regula entonces una vía excepcional que se genera cuando no existe una decisión de adecuación ni hay garantías adecuadas, ni tampoco se cuenta con la expresa autorización de la Autoridad de Control para realizar la transferencia internacional de datos.

Tratamiento Transfronterizo de Datos

Como se señaló anteriormente, el tratamiento transfronterizo de datos, que está regulado en el RGPD[523] es aquel realizado en el contexto de actividades de establecimientos en más de un Estado miembro de un responsable o un encargado del tratamiento en la Unión, si el responsable o el encargado está establecido en más de un Estado miembro. O aquel tratamiento de un único establecimiento de un responsable o un encargado del tratamiento en la Unión, pero que afecta sustancialmente o es probable que afecte sustancialmente a interesados en más de un Estado miembro. En definitiva, el tratamiento transfronterizo involucra las operaciones o tratamiento de datos al interior de las fronteras de la propia UE.

La expresión "afecte sustancialmente", a la que hace referencia el Reglamento, constituye un concepto jurídico indeterminado, por lo que para determinar su sentido y alcance el GT29, a propósito de la determinación de la autoridad de control principal, señaló que significa "influir o dejar una huella importante en algo de manera esencial". Por lo que el tratamiento de datos que no tenga un efecto esencial no constituye un tratamiento trasfronterizo, correspondiendo a cada autoridad de control determinar el sentido y alcance de la expresión "afecta sustancialmente". En efecto, el GT29 en el documento "Directrices para determinar la autoridad de control principal de un responsable o encargado del tratamiento"[524] dispone como factores a tener en cuenta: 1. Causa o probable causa de perjuicios, perdida o sufrimiento a las personas; 2. Tiene o es probable que tenga un efecto real en cuanto a la limitación de derechos o a la negación de una oportunidad; 3. Afecta o es probable que afecte la salud, el bienestar o la tranquilidad de las personas; 4. Afecta o es probable que afecte a la situación o circunstancias financieras o económicas de las personas; 5. Deja a las personas a merced de la discriminación o el tratamiento injusto; 6. Implica el análisis de categorías especiales de datos personales u otros datos intrusivos, en particular, los datos personales de los niños; 7. Produce o es probable que produzca un cambio significativo en el comportamiento de las personas; 8. Tienen

[523] Artículo 4 numero 23.

[524] Ver en: https://www.aec.es/conocimiento/documento/directrices-para-determinar-la-autoridad-de-control-principal-de-un-responsable-o-encargado-del-tratamiento/ consulta realizada el 19 de abril de 2021.

consecuencias improbables, imprevistas o indeseadas para las personas; 9. Produce vergüenza u otros resultados negativos, incluidos daños a la reputación; o 10. Implica el tratamiento de una amplia gama de datos personales.

Es, por consiguiente, la autoridad de control principal la que asume la responsabilidad del tratamiento transfronterizo de datos, tal como se desprende del apartado número 1 del artículo 56 del RGPD, que señala que la autoridad de control del establecimiento principal o del único establecimiento del responsable o del encargado del tratamiento será competente para actuar como autoridad de control principal para el tratamiento transfronterizo realizado por parte de dicho responsable o encargado, con arreglo al procedimiento de cooperación entre la autoridad de control principal y las demás autoridades de control interesadas.

El RGPD, en el artículo 4 referido a las definiciones, dispone en su N° 16 que el establecimiento principal abarca dos dimensiones: a) en lo que se refiere a un responsable del tratamiento con establecimientos en más de un Estado miembro, el lugar de su administración central en la Unión, salvo que las decisiones sobre los fines y los medios del tratamiento se tomen en otro establecimiento del responsable en la Unión y este último establecimiento tenga el poder de hacer aplicar tales decisiones, en cuyo caso el establecimiento que haya adoptado tales decisiones se considerará establecimiento principal; y b) en lo que se refiere a un encargado del tratamiento con establecimientos en más de un Estado miembro, el lugar de su administración central en la Unión o, si careciera de esta, el establecimiento del encargado en la Unión en el que se realicen las principales actividades de tratamiento en el contexto de las actividades de un establecimiento del encargado en la medida en que el encargado esté sujeto a obligaciones específicas con arreglo al Reglamento.

Troncoso Reigada[525] plantea, a propósito del tratamiento transfronterizo de datos personales, tres tipos regulados en el RGPD, los tratamientos puramente locales que solo afectan a un Estado miembro y que tiene la competencia de la autoridad local; los tratamientos transfronterizos que tiene la competencia de la autoridad de control del establecimiento principal; y los tratamientos mixtos que son los tratamientos transfronterizos con relevancia local. Añadiendo que "en el Reglamento definitivamente aprobado se señala que la autoridad de control no principal tendrá competencias en algunos supuestos como los tratamientos transfronterizos de impacto local que pueden darse en distintas circunstancias como son: los tratamientos efectuados únicamente en establecimientos situado en un determinado Estado; los tratamientos que resulten de ofertas de bienes y servicios específicamente dirigidos a un país concreto (de forma que al atribuir la competencia a la autoridad de control no principal se intenta preservar los derechos e intereses de los consumidores de dicho país); y los supuestos en que sea necesario aplicar la legislación nacional específica de un determinado Estado miembro (como sería, por ejemplo, la normativa de videovigilancia en el entorno laboral que se regula de forma muy diferente en España y en Alemania)".

Así entonces, las autoridades de control interesadas pueden participar en el proyecto de decisión que adopte la autoridad de control principal. De igual forma la autoridad de control del establecimiento principal o del único establecimiento del responsable o del encargado del tratamiento será competente para actuar como autoridad de control principal para el

[525] Troncoso Reigada, A. (2016), "Autoridades de Control Independientes", en "*Reglamento General de Protección de Datos, Hacia un nuevo modelo europeo de privacidad"*, director José Luis Piñar Mañas, Reus, Madrid, pp. 497-498.

tratamiento transfronterizo realizado por parte de dicho responsable o encargado, con arreglo al procedimiento de cooperación entre la autoridad de control principal y las demás autoridades de control interesadas.

En cualquier caso, cada autoridad de control será competente para tratar una reclamación que le sea presentada o una eventual infracción al RGPD, en el caso que se refiera a un establecimiento situado en su Estado miembro o solamente afecte de manera sustancial a interesados en su Estado miembro. Además, si la autoridad de control principal decide no tratar el caso, la autoridad de control que lo haya informado lo tratará bajo los criterios de asistencia mutua previstos en el artículo 61 del Reglamento y de operaciones conjuntas de las autoridades de control reguladas en el artículo 62 del RGPD.

Análisis comparado de la tipología de las Agencias de Protección de Datos

A continuación se analizarán los diseños con que se estructuran las entidades o autoridades de control en materia de protección de datos, en el sentido de si se configuran como agencias que únicamente regulan y promueven la protección de datos (modelo único) o además abordan el acceso a la información pública y la transparencia (modelo mixto), si son organismos unipersonales o colegiados, o si tienen autonomía o independencia o dependen de otro organismo superior del respectivo Estado donde se establecen, entre otros tópicos a estudiar.[526]

Hay autores como Troncoso Reigada, que plantean que el término "Agencia" no es el más adecuado para definir a una autoridad de control, ya que esa expresión, por ejemplo en el caso español, se usa para otros organismos públicos que carecen de independencia. Diferenciando la actividad que desarrollan las Autoridades de Protección de Datos y la de otros organismos que reciben la denominación de "Agencia", los cuales están dirigidos por Gerentes encargados de desarrollar determinados aspectos de gestión pública, pero no ejercen labores de control, no pueden imponer sanciones y no tienen la consideración de autoridad. De hecho, esas otras Agencias pueden ser creadas, modificadas o suprimidas por criterios de oportunidad política sin que su existencia esté justificada por la defensa de un derecho fundamental. Una expresión más adecuada a las funciones y a la organización que tienen es la de Autoridad de Protección de Datos, siguiendo la denominación empleada en otros países europeos y que fue asumida por la Carta de Derechos Fundamentales de la UE en su artículo 8.3.[527]

[526] Un interesante análisis en esta materia se encuentra en el Informe "Diseño de un Modelo Organizacional del Consejo Para La Transparencia en su nueva Función de Protección de Datos Personales", del Centro de Sistemas Públicos - Ingeniería Industrial, de la Universidad de Chile, de 18 de mayo de 2010, donde se analizan las agencias encargadas de la protección de datos de Canadá, Italia, Inglaterra, Alemania, Portugal, Finlandia, España y Uruguay. A lo largo de este trabajo y donde sea posible se hará referencia a lo señalado respecto de esos países, que a la fecha de este trabajo se encuentre vigente. Ver en: http://www.sistemaspublicos.cl/wp-content/uploads/files_mf/1277938127_6_1_1_9_archivo.pdf consulta realizada el 19 de junio de 2020.

[527] Pauner C. y Tomás B. (2009), "Las Agencias de Protección de Datos como Administración Independiente", en "*Las Administraciones Independientes*", Tirant Lo Blanch, Valencia, pp. 27-216.

1. Modelo único o mixto

Esta categorización permitirá revisar si en los diferentes países la regulación de la protección de datos se encuentra radicada en una agencia que posee esa única función, lo que se denominará modelo único, o concentra además la función de garantizar el acceso a la información pública, que se denominará modelo mixto. Para lo cual se distinguirá entre los países que integran la Unión Europea, los países del OCDE y los países que integran la Red Iberoamérica de Protección de Datos.

Países de la Unión Europea

Para realizar este análisis se consideraron 28 países, que son los que integran la Unión Europea[528] (para estos efectos se consideró también el Reino Unido) y que cuentan con agencias encargadas para la protección de datos.

A continuación, un cuadro que muestra el país, la respectiva autoridad de control, el año en que se crea la entidad, si esta se estructura sobre un modelo único que solo regula la protección de datos o un modelo mixto que además regula el derecho de acceso a la información pública (DAIP) y si su alcance afecta al sector público, privado o a ambos:

Cuadro N° 3:

País	**Autoridad de Control**	**Año de creación**	**Modelo único/mixto**	**Ámbito de aplicación**
Alemania	Comisionado General para la Protección de Datos y Libertad de Información	1978, en el año 2006 asume funciones en protección de datos	Mixto: Protección de datos personales y Acceso a Información Pública	Sobre entidades públicas y sector privado corresponde a las autoridades federales salvo industrias de telecomunicaciones y servicios postales
Austria	Autoridad de protección de datos, que es a sucesora de la Comisión de Protección de Datos creada en 1978	2014	Único: Protección de Datos	Sobre entidades públicas y privadas, pero la tutela de los derechos ARCO se entrega a los tribunales o Cortes

[528] Ver: https://ec.europa.eu/justice/article-29/structure/data-protection-authorities/index_en.htm consulta realizada el 09 de junio de 2020.

Bélgica	Autoridad de Protección de datos	1992	Único: Protección de Datos	Sobre entidades públicas y privadas
Bulgaria	Comisión de Protección de Datos Personales	2002	Único: Protección de Datos	Sobre entidades públicas y privadas
Croacia	Agencia Croata de Protección de Datos	2003	Único: Protección de Datos	Sobre entidades públicas y privadas
Chipre	Comisionado de Protección de Datos Personales	2001	Único: Protección de Datos	Sobre entidades públicas y privadas
Dinamarca	Agencia Danesa de Protección de Datos	2000	Único: Protección de Datos	Sobre entidades públicas y privadas
Estonia	Inspector de Protección de Datos de Estonia	2008	Mixto: Protección de datos personales y Acceso a Información Pública	Sobre entidades públicas y privadas
España[529]	Agencia Española de Protección de Datos[530]	1994	Único: Protección de Datos	Sobre entidades públicas y privadas
Eslovenia	Comisionado de Información	2005	Mixto: Protección de datos personales y Acceso a Información Pública	Sobre entidades públicas y privadas
Eslovaquia	Oficina de Protección de Datos	2013	Único: Protección de Datos	Sobre entidades públicas y privadas
Finlandia	Oficina del Defensor de Datos Personales[531]	1987	Único: Protección de Datos	Sobre entidades públicas y privadas

[529] Es importante señalar que la Agencia Española de Protección de Datos es la autoridad nacional o según el RGPD la autoridad de control principal y su ámbito de regulación abarca tanto al sector público como privado. Sin embrago, el ordenamiento jurídico español también reconoce a las denominadas autoridades autonómicas en la materia, donde se distingue la Autoridad Catalana de Protección de Datos y la Agencia Vasca de Protección de Datos, que regulan el tratamiento de datos en el sector público de sus respectivos territorios y que se configuraran bajo el denominado modelo único. También y de manera más reciente se ha creado el Consejo de Transparencia y Protección de Datos de Andalucía que regula el tratamiento de datos de carácter personal en el sector público y el derecho de acceso a la información pública, en el territorio de su competencia, eso sí, a diferencia de las otras autoridades autonómicas en la materia se estructura bajo el modelo mixto.

[530] La AEPD es un Ente de Derecho público, con personalidad jurídica propia y plena capacidad pública y privada, que actúa con plena independencia de las Administraciones Públicas en el ejercicio de sus funciones.

[531] El enfoque de la autoridad de control, antes del RGPD, era más bien el de una institución que privilegia la educación y promoción en protección de datos personales.

Francia	Comisión Nacional de la Información y la Libertad	1978	Único: Protección de Datos	Sobre entidades públicas y privadas
Grecia	Autoridad Griega de Protección de Datos	1997	Único: Protección de Datos	Sobre entidades públicas y privadas
Hungría	Autoridad Nacional de Protección de Datos y Libertad de Información	2011	Mixto: Protección de datos personales y Acceso a Información Pública	Sobre entidades públicas y privadas
Holanda	Autoridad Holandesa de Protección de Datos	1989	Único: Protección de Datos	Sobre entidades públicas y privadas
Irlanda	Comisión de Protección de Datos	1988	Único: Protección de Datos	Sobre entidades públicas y privadas
Italia	Autoridad Garante de Protección de Datos Personales[532]	1997	Único: Protección de Datos	Sobre entidades públicas y privadas
Latvia	Inspector Estatal de Datos Personales	2001	Único: Protección de Datos	Sobre entidades públicas y privadas
Lituania	Inspector Personal de Datos Personales	1997	Único: Protección de Datos	Sobre entidades públicas y privadas
Luxemburgo	Comisión Nacional de Protección de Datos	2002	Único: Protección de Datos	Sobre entidades públicas y privadas
Malta	Comisionado de Información y Protección de Datos	2001	Mixto: Protección de datos personales y Acceso a Información Pública	Sobre entidades públicas y privadas
Polonia	Inspector General para la Protección de Datos Personales	1997	Único: Protección de Datos	Sobre entidades públicas y privadas

[532] Uno de los elementos a destacar de la experiencia italiana es la suscripción a un código de ética por parte de los consejeros de la Autoridad de Control lo que ha prevenido situaciones de conflicto de intereses de las autoridades y ha fortalecido la legitimidad de sus resoluciones. Cabe señalar que la autoridad de control, si bien tiene facultades sancionadoras y en los casos en los que el Consejo considera necesario puede aplicar multas diferenciadas a los infractores, antes del RGPD sus potestades inspectivas y fiscalizadoras no eran del todo eficientes.

Portugal	Comisión Nacional de Protección de Datos[533]	1994	Único: Protección de Datos	Sobre entidades públicas y privadas
Rumania	Autoridad Supervisora Nacional de Protección de Datos	2005	Único: Protección de Datos	Sobre entidades públicas y privadas
Suecia	Autoridad Sueca de Protección de Datos	2007	Único: Protección de Datos	Sobre entidades públicas y privadas
Reino Unido[534]	Oficina del Comisionado de Información[535]	1998	Mixto: Protección de datos personales y Acceso a Información Pública	Sobre entidades públicas y privadas
República Checa	Oficina de Protección de Datos Personales	2000	Único: Protección de Datos	Sobre entidades públicas y privadas

Fuente: elaboración propia.

Como se observa del cuadro anterior, la mayoría de los países de la Unión estructuran sus agencias para la regulación de la protección de datos bajo el modelo único, es decir abordan, regulan y promueven exclusivamente la protección de datos; en efecto de un total de 28 Estados miembros, veintidós estructuran una autoridad de control encargada exclusivamente de la protección de datos de carácter personal.

En contrapartida, solo seis países del bloque estructuran sus entidades de control bajo el modelo mixto, es decir, sus respectivas agencias regulan conjuntamente la protección de datos con el derecho de acceso a la información pública y la transparencia. Son el caso de Alemania, Reino Unido, Hungría, Eslovenia, Estonia y Malta[536].

[533] Es una entidad administrativa independiente con poderes de autoridad, que funciona junto con la Asamblea de la República. Tiene facultades sancionadoras (multas y posibilidad de denuncias al Ministerio Público), y de fiscalización. Sus decisiones son obligatorias y susceptibles de reparación y denuncia ante el Tribunal Administrativo Central. En el caso de los procesos de contra coordinación, las decisiones de la Comisión son llevadas a los tribunales de pequeña instancia penal o a los tribunales competentes.

[534] Hay que considerar que, si bien el Reino Unido ya no forma parte de la UE, hasta el 31 de diciembre del año 2020 se estuvo en un periodo de transición que determinara la futura relación entre británicos y europeos. Durante ese periodo de transición, Reino Unido siguió acatando las normas de la UE y contribuyendo a su presupuesto, de hecho, permanece en la unión aduanera y en el mercado único, pero queda fuera de las instituciones políticas y del Parlamento europeo.

[535] El ICO es un organismo independiente y tiene atribuciones para la protección de datos en todo el Reino Unido, antes del RGPD sus acciones para garantizar la libertad de información solo tienen efecto para Inglaterra, Irlanda del Norte y Gales.

[536] Los países que adoptan el modelo único representan en su conjunto el 61.1% del PIB de la UE, y los que adoptan el sistema mixto (considerando aún al Reino Unido) representan un PIB del 36.6% del Bloque, según información extraída de: https://ec.europa.eu/eurostat/web/products-eurostat-news/-/DDN-20180511-1?inheritRedirect=true consulta realizada el 11 de junio de 2020.

Es importante consignar que con la entrada en vigor del Reglamento Europeo de Protección de Datos 2016/679, los países debieron adaptar sus legislaciones internas para armonizarlas con esa normativa general, no obstante, no alteraron la forma en que se estructura su agencia de control, por cuanto ambos modelos, único y mixto, aseguran el estándar de cumplimiento exigido por el RGPD respecto de la autoridad de control.

Hay que señalar también que, en los Estados miembros de la Unión Europea, los Directores de las Autoridades de Protección de Datos tienen reconocido incluso el rango de Ministro (Polonia o la República Checa) o Presidente del Tribunal Supremo (Italia), siendo en otros casos Comisionados Parlamentarios equivalentes al Defensor del Pueblo (Finlandia o Hungría) o son reconocidos entre las Altas Autoridades del Estado (Francia). La importancia de la autoridad de control en las instituciones comunitarias se expresa también en que el Supervisor Europeo de Protección de Datos tiene un rango equivalente a un Juez del Tribunal de Justicia de las Comunidades Europeas.

Del cuadro N°3 también es posible extraer que quince autoridades de control se crean desde la década del dos mil en adelante. Además, en el caso de la entidad alemana, el Comisionado General para la Protección de Datos y la Libertad de Información, creado en el año 1978, asume en el año 2006 la regulación en materia de protección de datos de carácter personal. Del mismo cuadro también es posible colegir que la entidad francesa, la Comisión Nacional de la Información y la Libertad, creada en 1978, es la más antigua agencia de control de protección de datos vigente hasta nuestros días, y la más nueva es la Oficina de Protección de Datos de Eslovaquia, creada el año 2013.

Finalmente, en su mayoría, las autoridades de control regulan el tratamiento de datos sobre el sector público y privado con las excepciones de la entidad Alemana que regulan a las entidades públicas, ya que el sector privado corresponde a las autoridades federales, salvo las relacionadas con las industrias de telecomunicaciones y servicios postales; y la entidad Austríaca, que si bien regula a las entidades públicas y privadas, la tutela de los denominados derechos ARCO se entrega a los tribunales o Cortes de dicho país.

Países de la *Organización para la Cooperación y el Desarrollo Económicos* - OCDE

Entre los países[537] que integran la OCDE[538], se observa una prevalencia del sistema único, es decir, de entidades que solamente se abocan a la regulación de la protección de datos. Respecto de los países europeos que integran este bloque, el panorama es básicamente el mismo que el descrito en el cuadro anterior, ya que como se señaló, la mayoría adhieren al modelo único, considerando incluso los países europeos que no integran la OCDE[539].

Por lo señalado, de los 27 países de Europa que integran el bloque OCDE, 22 adoptan un modelo único, lo que porcentualmente representa un 81.4%, versus un 19.6% que opta por el

[537] La Organización para la Cooperación y el Desarrollo Económico (OCDE) es un organismo de cooperación internacional, compuesto por 38 Estados, su objetivo es coordinar sus políticas económicas y sociales. La OCDE fue fundada en 1961 y su sede central se encuentra en el Château de la Muette en París, Francia. Los idiomas oficiales de la entidad son el francés y el inglés. En la OCDE, los representantes de los países miembros se reúnen para intercambiar información y armonizar políticas con el objetivo de maximizar su crecimiento económico y colaborar a su desarrollo y al de los países no miembros. La OCDE es la sucesora de la Organización Europea para la Cooperación Económica (OECE), resultado del Plan Marshall y de la Conferencia de los Dieciséis (Conferencia de Cooperación Económica Europea), que existió entre 1948 y 1960 y que fue liderada por el francés Robert Marjolin. Su objetivo era el establecimiento de una organización permanente encargada, en primer lugar, de garantizar la puesta en marcha de un programa de recuperación conjunta (Plan Marshall) y, en particular, de supervisar la distribución de la ayuda.

La organización nació cuando veinte países, tanto de América del Norte como de Europa, se adhirieron a la "Convención de la OCDE" llevada a cabo en París el 14 de diciembre de 1960. Actualmente la OCDE se ha constituido en uno de los foros mundiales más influyentes, en el que se analizan y se establecen orientaciones sobre temas de relevancia internacional como economía, educación y medio ambiente. Los países miembros se comprometen a aplicar los principios de liberalización, no discriminación, trato nacional y trato equivalente. El principal requisito para ser país miembro de la OCDE es liberalizar progresivamente los movimientos de capitales y de servicios.

[538] En mayo de 2007, el Consejo ministerial de la OCDE comenzó a analizar y a discutir el acceso de Chile, Eslovenia, Estonia, Costa Rica, Israel y Rusia a la organización. Chile y Eslovenia fueron los dos únicos países en completar el proceso de incorporación en menos de un año. El 15 de diciembre de 2009, la OCDE anunció oficialmente la invitación a Chile a formar parte de la organización como miembro pleno. El 11 de enero de 2010, se efectuó la ceremonia de firma del convenio de adhesión en el Palacio de La Moneda en Santiago, con la presencia del entonces Secretario General de la Organización, Ángel Gurría, y en ese entonces la presidenta de Chile, Michelle Bachelet. El 10 de marzo del mismo año, el Congreso ratificó el acuerdo y, posteriormente, el gobierno de Chile depositó el instrumento de adhesión con el gobierno de Francia, en una ceremonia efectuada en la sede del Ministerio de Relaciones Exteriores de Francia en París, el 7 de mayo de 2010. Con este último paso, Chile se convirtió oficialmente en el 31er miembro de la organización. El 10 de mayo de 2010, la OCDE anunció oficialmente la invitación a Eslovenia, Estonia e Israel a formar parte de la organización como miembros plenos. Eslovenia ingresó oficialmente al grupo el 21 de julio de 2010, Israel lo hizo el 7 de septiembre del mismo año y Estonia, el 9 de diciembre de 2010. El 2 de junio de 2016, se ratificó el ingreso a la organización de Letonia, que depositó oficialmente el instrumento de adhesión el 1 de julio del mismo año y se convirtió en el 35° país miembro. En mayo de 2018, Colombia y Lituania fueron invitados a formar parte como miembros plenos de la organización. La membrecía de Colombia entró en vigor el 28 de abril de 2020, después de haber tomado las medidas apropiadas a nivel nacional para adherirse a la Convención de la OCDE y depositar su instrumento de adhesión ante el gobierno francés, el depositario de la Convención. La adhesión de Colombia amplió la membrecía de la OCDE a 37 países. El 15 de mayo de 2020 la OCDE invitó formalmente a Costa Rica para ser el 38º miembro, adhesión que debe ser ratificada legislativamente en dicho país.

[539] Caso de Noruega, Turquía, Suiza, Islandia

sistema mixto, es decir, donde las agencias de control regulan conjuntamente el derecho de acceso a la información y la protección de datos personales.

Por su parte, en el caso de los países de América[540] integrantes de la OCDE y que cuentan con autoridades de control en la materia, Canadá adopta un modelo único[541], mientras México uno mixto, a los que se suma Colombia con su reciente incorporación al bloque OCDE, donde la Superintendencia de Industria y Comercio, que si bien regula otras materias tales como protección del consumidor, propiedad industrial y protección a la competencia, para estos efectos es un modelo único, por cuanto aborda exclusivamente la protección de datos de carácter personal y no el derecho de acceso a la información pública.

En el caso de Oceanía, Australia opta por un modelo mixto, mientras que Nueva Zelanda por un modelo único.

En el caso de Asía, Corea y Japón adoptan un modelo mixto, por lo que todos los países de ese continente que integran la OCDE[542] tienen entidades de control que abordan conjuntamente el derecho de acceso a la información pública y la protección de datos de carácter personal.

También hay que tener en cuenta, entre las institucionalidades más recientes en materia de protección de datos el caso de Turquía, que adopta modelo único. Lo mismo ocurre con Israel, cuya autoridad de control se crea en el año 1981.

A continuación, se expone un cuadro de los países OCDE, que no incluye a los países de la UE listados en el cuadro número tres.

Cuadro N° 4:

País	**Autoridad de Control**	**Año de creación**	**Modelo único/mixto**	**Ámbito de aplicación**
Australia	Oficina del Comisionado de Información	2010	Mixto: Protección de datos personales y Acceso a Información Pública	Sobre entidades públicas y privadas
Canadá[543]	Oficina del Comisionado de	1983	Mixto: Protección de Datos y Acceso	Sobre entidades públicas y privadas

[540] Se excluyen de la muestra Chile y EE. UU. al no contar oficialmente con una institucionalidad (agencia) encargada específicamente de la protección de datos personales. Para una visión de las diferencias de los sistemas de PDP entre EE. UU y Europa véase: Bush, A. (2013), "The Regulation of Privacy, Handbook on the Politics of Regulation (edited by David Levi-Faur. Edward Elgar), *Publishing Limited*, ciudad, pp. 227-237.

[541] El modelo único opera a nivel federal, mientras que a nivel estatal la institucionalidad es de carácter mixto.

[542] China, el país más grande del continente asiático es adherente al bloque y presta cooperación reforzada.

[543] En Canadá, la regulación y garantía de la transparencia y acceso a la información, así como la protección de datos personales, están regidas por dos instituciones distintas: la Oficina del Comisionado de Información (OIC), para el primer caso, y la Oficina del Comisionado de Privacidad de Canadá (OCP), para el segundo. La OCP de Canadá se encarga de regular la protección de los datos personales tanto en instituciones del gobierno como en las empresas privadas en todo el país. Un aspecto para destacar en la experiencia canadiense de institucionalización de la protección de datos es el establecimiento de la conciliación y mediación, lo que ha

	Privacidad de Canadá		a Información Pública a nivel estatal a nivel federal es un modelo único	
Islandia	Autoridad Islandesa de Protección de Datos	2000	Único: Protección de Datos	Sobre entidades públicas y privadas
Israel	Autoridad de Protección a la Privacidad	1981	Único: Protección de Datos	Sobre entidades públicas y privadas
Japón	Comisión de Protección de Información Personal	2016	Único: Protección de Datos	Sobre entidades públicas y privadas
Corea del Sur	Comisión de Protección de Información Personal	2011	Único: Protección de Datos	Sobre entidades públicas y privadas
México	Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos	2010	Mixto: Protección de datos personales y Acceso a Información Pública	Sobre entidades públicas y privadas
Noruega	Autoridad Noruega de Protección de Datos	1980	Único: Protección de Datos	Sobre entidades públicas y privadas
Suiza	Comisionado Federal de Protección de Datos e Información	2006	Mixto: Protección de datos personales y Acceso a Información Pública	Sobre entidades públicas y privadas
Turquía	Autoridad Nacional de Protección de Datos	2016	Único: Protección de Datos	Sobre entidades públicas y privadas

Fuente: elaboración propia.

Si bien Chile y EE. UU integran la OCDE, estos países no cuentan con entidades de control encargadas directamente de la protección de datos. En el caso norteamericano la *Federal Trade Commission* FTC o Comisión Federal de Comercio[544], ejerce atribuciones sobre entidades

permitido reducir significativamente el número de denuncias y procesos sancionatorios formales ante tribunales ordinarios externos.

[544] La Misión de la FTC es "Prevenir las prácticas comerciales anticompetitivas, engañosas o desleales hacia los consumidores; mejorar el nivel de información de las opciones disponibles para los consumidores y aumentar el grado de comprensión del proceso competitivo por parte del público; y cumplir con estos objetivos sin imponer una carga indebida sobre la actividad comercial legítima". Y sus objetivos estratégicos son: "1. Proteger a los

comerciales, relacionadas con áreas específicas como el telemarketing, correos electrónicos comerciales y privacidad de niños, así como divulgación inadecuada de información. La FTC también regula las prácticas comerciales desleales y las acciones para impedir la recopilación inadecuada de datos.

En el caso de Chile, actualmente está en tramitación (en primer trámite constitucional) el proyecto de ley[545] que modifica la Ley N° 19.628 sobre protección a la vida privada, que le asigna la regulación y control de la protección de datos de carácter personal al Consejo para la Transparencia[546], cuya misión es " Contribuir a fortalecer la democracia en Chile a través de la rendición de cuentas y el control social, al garantizar el acceso a la información pública, la transparencia y la protección de datos personales" siendo sus objetivos: Promover y difundir el principio de transparencia, el derecho de acceso a la información pública y la protección de datos personales como herramientas de la rendición de cuentas de autoridades y de control social, así como favorecer el ejercicio de otros derechos; Garantizar el principio de transparencia y el derecho de acceso a la información pública velando por el adecuado cumplimiento de la protección de datos personales, y fiscalizar el cumplimiento de las normas de transparencia, el derecho de acceso a la información y la protección de datos personales aplicando las sanciones que corresponda en caso de incumplimiento.

Si bien dentro de las funciones y objetivos del Consejo para la Transparencia se encuentra la protección de datos personales, esta es una función residual en su quehacer. En efecto, la letra m) del artículo 33 de la Ley 20.285[547] le reconoce la atribución de velar por el adecuado cumplimiento de la Ley 19.628, de protección de datos de carácter personal, por parte de los órganos de la Administración del Estado, sin embargo, esta resulta insuficiente para que se constituya como la autoridad de control, ya que su ámbito de control solo se reduce a las entidades públicas, sin tener competencia sobre las entidades privadas que realizan algún tipo de tratamiento de datos de carácter personal, además, desde el punto de vista práctico, su principal actividad esta direccionada a la promoción y regulación del derecho de acceso a la información pública y a la promoción de la transparencia, así ha sido desde su creación en el año 2009.

consumidores: prevenir el fraude, el engaño y las prácticas comerciales desleales en el mercado; 2. Mantener la competencia: prevenir fusiones anticompetitivas y otras prácticas comerciales anticompetitivas en el mercado y 3. Promover el buen desempeño: promover el buen desempeño de la FTC a través de la excelencia organizacional, individual y de gestión". Según consulta efectuada a su página web: https://www.ftc.gov/es/acerca-de-la-ftc el 12 de junio de 2020.

[545] Refundidos los Boletines Legislativos números 11.144 y 11.092

[546] El Consejo para la Transparencia (CPLT) es una corporación autónoma de derecho público, con personalidad jurídica y patrimonio propio, creado por la Ley de Transparencia de la Función Pública y de Acceso a la Información de la Administración del Estado n° 20.285. Su principal labor es velar por el buen cumplimiento de dicha ley, la que fue promulgada el 20 de agosto de 2008 y entra en vigor el 20 de abril de 2009.

[547] Ley sobre Acceso a la Información Pública, publicada en el Diario Oficial el 20 de agosto del año 2008.

Países miembros de la Red Iberoamericana de Protección de Datos

La Red Iberoamericana de Protección de Datos publicó en junio de 2017 el documento "Estándares de protección de datos personales para los Estados iberoamericanos"[548], los que constituyen un conjunto de directrices orientadoras que contribuyen a la emisión de iniciativas regulatorias de protección de datos personales en la región iberoamericana, especialmente para aquellos países que aún no cuentan con estas regulaciones, o en su caso, sirven como referente para la modernización y actualización de las legislaciones existentes[549].

Estos Estándares establecen en su considerando 24, a propósito de las autoridades de control en la materia que: "Admitiendo la imperiosa necesidad de que cada Estado Iberoamericano cuente con una autoridad de control independiente e imparcial en sus potestades cuyas decisiones únicamente puedan ser recurribles por el control judicial, ajena a toda influencia externa, con facultades de supervisión e investigación en materia de protección de datos personales y encargada de vigilar el cumplimiento de la legislación nacional en la materia, la cual esté dotada de recursos humanos y materiales suficientes para garantizar el ejercicio de sus poderes y el desempeño efectivo de sus funciones".

Por su parte, si bien en el ámbito latinoamericano no existe todavía un instrumento supranacional, vinculante, que reconozca y que regule el derecho a la protección de datos personales, sí ha sido reconocido en instrumentos de *soft law*, como la declaración de Santa Cruz de la Sierra, adoptada en 2003, al final de una cumbre iberoamericana de Jefes de Estado, que en su numeral 45 establece: "Asimismo somos conscientes de que la protección de datos personales es un derecho fundamental de las personas y destacamos la importancia de las iniciativas regulatorias iberoamericanas para proteger la privacidad de los ciudadanos contenidas en la Declaración de La Antigua por la que se crea la Red Iberoamericana de Protección de Datos, abierta a todos los países de nuestra Comunidad".[550]

A continuación, se verá cómo se constituyen las agencias o autoridades de control en materia de protección de datos de carácter personal entre los países que integran la Red Iberoamericana de Protección de datos, la que está integrada por doce países a saber: Andorra, Argentina, Brasil, Chile, Colombia, Costa Rica, España, México, Panamá, Perú, Portugal y Uruguay, además de las siguientes entidades que integran la Red en calidad de observadores. De México: el Instituto Coahuilense de Acceso a la Información Pública (ICAI), el Instituto de Transparencia, Información Pública y Protección de Datos Personales del Estado de Jalisco (ITEI), el Instituto de Acceso a la Información Pública del Estado de Chiapas

[548] Ver en: https://www.redipd.org/sites/default/files/inline-files/Estandares_Esp_Con_logo_RIPD.pdf

[549] En el marco del XV Encuentro Iberoamericano de Protección de Datos, la Red Iberoamericana de Protección de Datos (RIPD) aprueba y presenta oficialmente el señalado documento, dando cumplimiento a un objetivo planteado por todas las entidades integrantes de la Red, así como a uno de los acuerdos adoptados en la XXV Cumbre Iberoamericana de Jefes de Estado y de Gobierno, celebrada el 28 y 29 de octubre de 2016 en Colombia, relacionado con solicitar a la Red la elaboración de una propuesta para la cooperación efectiva relacionada con la protección de datos personales y privacidad. El texto trata de dar respuesta a uno de los ejes de la estrategia acordada por la RIPD en noviembre de 2016 en Montevideo, plasmada en el documento "RIPD 2020", consistente en "impulsar y contribuir al fortalecimiento y adecuación de los procesos regulatorios en la región, mediante la elaboración de directrices que sirvan de parámetro para futuras regulaciones o para la revisión de las existentes".

[550] Ver en: http://iccnow.org/documents/decla_Santa_Cruz_de_la_Sierra.pdf

(IAIPCHIAPAS), el Instituto Veracruzano de Acceso a la Información y Protección de Datos Personales (IVAI) y la Comisión de Transparencia y Acceso a la Información del Estado de Nuevo León (CTAINL).

De Argentina, la Defensoría del Pueblo de la Ciudad de Buenos Aires; de la República de Cabo Verde, la Comissão Nacional De Protecçao De Dados (CNPD); de la República del Salvador, el Instituto de Acceso a la Información Pública (IAIP); de la República de Guatemala, la Procuraduría de Derechos Humanos; de la República de Honduras, el Instituto de Acceso a la Información Pública (IAIP); de Ecuador, la Función de Transparencia y Control Social (FTCS); de Paraguay, la Secretaría de la Función Pública; de la República Democrática de Santo Tomé y Príncipe, la Agência Nacional de Protecção de Dados Pessoais de Santo Tomé e Príncipe (ANPDP); de República Dominicana, la Dirección General de Ética e Integridad Gubernamental (DIGEIG) y de la Unión Europea, el Comité Consultivo del Convenio 108-Consejo de Europa[551].

En el siguiente cuadro se muestra la forma en que se estructuran las autoridades de control en protección de datos de carácter personal que integran la Red Iberoamericana de Protección de Datos, con la excepción de Chile, México, Portugal y España, ya que las autoridades de control de estos tres últimos países fueron precedentemente expuestas, y en el caso chileno, como ya se señaló, no existe una autoridad de control en la materia.

Cuadro N° 5

País	Autoridad de Control	Año de creación	Modelo único/mixto	Ámbito de aplicación
Andorra	Agencia Andorrana de Protección de Datos	2013	Único: Protección de Datos	Sobre entidades públicas y privadas
Argentina	Agencia de Acceso a la Información Pública	2017	Mixto: Protección de datos personales y Acceso a Información Pública	Sobre entidades públicas y privadas
Brasil	Autoridad Nacional de Protección de Datos (ANPD)	2020	Único: Protección de Datos	Sobre entidades públicas y privadas
Uruguay	Agencia para el Desarrollo del Gobierno de Gestión Electrónica y la Sociedad de la información y del	2008	Mixto: Protección de datos personales y Acceso a Información Pública	Sobre entidades públicas y privadas

[551] Ver: https://www.redipd.org/es/la-red/entidades-acreditadas consulta realizada el 12 de junio de 2020.

	Conocimiento (AGESIC)[552]			
Colombia	Superintendencia de Industria y Comercio[553]	2011	Único: Protección de Datos	Sobre entidades públicas y privadas
Panamá	Autoridad Nacional de Transparencia y Acceso a la Información	2013	Mixto: Protección de datos personales y Acceso a Información Pública	Sobre entidades públicas y privadas
Perú	Dirección General de Transparencia, Acceso a la Información Pública y Protección de Datos Personales[554]	2013	Mixto: Protección de datos personales y Acceso a Información Pública	Sobre entidades públicas y privadas
Costa Rica	Agencia de Protección de Datos de los Habitantes	2011	Único: Protección de Datos	Sobre entidades públicas y privadas

Fuente: elaboración propia.

De lo señalado, es posible concluir que entre los países que integran la Red Iberoamericana de Protección de Datos – RIPD, sin considerar a Chile, cinco adhieren a un modelo único, como es el caso de Andorra, España (esta figura en el cuadro N° 1), Brasil, Colombia y Costa Rica, y cinco países estructuran sus autoridades de control bajo el modelo mixto, como es el caso de Argentina, México, Panamá, Perú y Uruguay. Por consiguiente, se muestra un total equilibrio en relación con la forma de estructuración de las agencias de control, a diferencia de lo que ocurre en la UE y en la OCDE.

[552] Esa función mixta la realiza a través de la Unidad Reguladora y de Control de Datos Personales y de la Unidad de Acceso a la Información Pública.

[553] A través de la Delegatura de Protección de Datos Personales.

[554] El Título VI "Autoridad Nacional de Protección de Datos Personales de la Ley N° 29.733 del Perú, dispone en su artículo 32, sobre el Órgano competente y régimen jurídico, que: "El Ministerio de Justicia, a través de la Dirección Nacional de Justicia, es la Autoridad Nacional de Protección de Datos Personales. Para el adecuado desempeño de sus funciones, puede crear oficinas en todo el país. La Autoridad Nacional de Protección de Datos Personales se rige por lo dispuesto en esta Ley, en su reglamento y en los artículos pertinentes del Reglamento de Organización y Funciones del Ministerio de Justicia. Corresponde a la Autoridad Nacional de Protección de Datos Personales realizar todas las acciones necesarias para el cumplimiento del objeto y demás disposiciones de la presente Ley y de su reglamento. Para tal efecto, goza de potestad sancionadora, de conformidad con la Ley 27444, Ley del Procedimiento Administrativo General, o la que haga sus veces, así como de potestad coactiva, de conformidad con la Ley 26979, Ley de Procedimiento de Ejecución Coactiva, o la que haga sus veces. La Autoridad Nacional de Protección de Datos Personales debe presentar periódicamente un informe sobre sus actividades al Ministro de Justicia. Para el cumplimiento de sus funciones, la Autoridad Nacional de Protección de Datos Personales cuenta con el apoyo y asesoramiento técnico de la Oficina Nacional de Gobierno Electrónico e Informática (ONGEI) de la Presidencia del Consejo de Ministros, o la que haga sus veces".

Otro aspecto para considerar es que, salvo España y Uruguay, los otros países estructuraron sus agencias de control en materia de protección de datos personales dentro de la última década. Sin embargo, pereciera que la adhesión a un modelo mixto a nivel iberoamericano ha tenido un mayor desarrollo en los últimos años. En efecto, México desde el año 2010 mediante la Ley Federal de Protección de Datos Personales en posesión de particulares, agregó a las funciones que hasta ese entonces desarrollaba el Instituto Federal de Acceso a la Información en materia de acceso a la información, las de protección de datos personales[555]. De igual forma, Argentina en el año 2016, mediante la Ley N° 27.275 creó la Agencia de Acceso a la Información Pública, a quien atribuyó conjuntamente las funciones de garantizar el acceso a la información pública y la protección de datos personales[556]. En Brasil, en agosto de 2018, se aprueba la Ley General de Protección de Datos Personales N° 13.709[557], que entraría en vigor en agosto de 2020, ya que estableció una vacancia legal de 24 meses, plazo que nuevamente fue postergado parcialmente hasta el 3 de mayo de 2021, mediante la Medida Provisional N° 959/2020, publicada en el Diario Oficial de la Unión el 29 de abril[558]. Es una postergación parcial por cuanto se mantuvo la entrada en vigor para agosto del año 2020 para algunos de sus articulados, como por ejemplo el artículo 55 que regula la creación de la Autoridad Nacional para la Protección de Datos Personales -ANPD, según lo previsto en el artículo 65[559] de la mencionada

[555] Por esta modificación el organismo pasó a denominarse Instituto Federal de Acceso a la Información y Protección de Datos. Posteriormente en el año 2016, en virtud de la modificación introducida por la Ley General de Acceso a la información, pasó de denominarse Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos.

[556] Antes de la dictación de la Ley N° 27.275, la institucionalidad en protección de datos personales era de carácter única, ya que dicha función estaba radicada exclusivamente en la Dirección Nacional de Protección de Datos, reglamentada mediante Decreto N° 1558/2001. En cualquier caso, las funciones y atribuciones del órgano de control están previstas en la Ley N° 25.326 del 2 de noviembre del año 2000, que se encuentra vigente y que en su artículo 29 señala: "1. El órgano de control deberá realizar todas las acciones necesarias para el cumplimiento de los objetivos y demás disposiciones de la presente ley. A tales efectos tendrá las siguientes funciones y atribuciones: a) Asistir y asesorar a las personas que lo requieran acerca de los alcances de la presente y de los medios legales de que disponen para la defensa de los derechos que ésta garantiza; b) Dictar las normas y reglamentaciones que se deben observar en el desarrollo de las actividades comprendidas por esta ley; c) Realizar un censo de archivos, registros o bancos de datos alcanzados por la ley y mantener el registro permanente de los mismos; d) Controlar la observancia de las normas sobre integridad y seguridad de datos por parte de los archivos, registros o bancos de datos. A tal efecto podrá solicitar autorización judicial para acceder a locales, equipos, o programas de tratamiento de datos a fin de verificar infracciones al cumplimiento de la presente ley; e) Solicitar información a las entidades públicas y privadas, las que deberán proporcionar los antecedentes, documentos, programas u otros elementos relativos al tratamiento de los datos personales que se le requieran. En estos casos, la autoridad deberá garantizar la seguridad y confidencialidad de la información y elementos suministrados; f) Imponer las sanciones administrativas que en su caso correspondan por violación a las normas de la presente ley y de las reglamentaciones que se dicten en su consecuencia; g) Constituirse en querellante en las acciones penales que se promovieran por violaciones a la presente ley; h) Controlar el cumplimiento de los requisitos y garantías que deben reunir los archivos o bancos de datos privados destinados a suministrar informes, para obtener la correspondiente inscripción en el Registro creado por esta ley".

[557]Ver en: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709compilado.htm. Consulta realizada el 22 de julio de 2020.

[558]Ver en: http://www.in.gov.br/web/dou/-/medida-provisoria-n-959-de-29-de-abril-de-2020-254499639. Consulta realizada el 22 de julio de 2020.

[559]Esta Ley entra en vigencia: I - 28 de diciembre de 2018, en relación con los arts. 55-A, 55-B, 55-C, 55-D, 55-E, 55-F, 55-G, 55-H, 55-I, 55-J, 55-K, 55-L, 58- A y 58-B; y IA - 1 de agosto de 2021, en relación con los arts. 52,

ley, no pudiendo eso sí, esta entidad aplicar sanción alguna hasta el 3 de mayo de 2021. La Autoridad Nacional para la Protección de Datos ANPD adhiere a un modelo único donde regula exclusivamente la protección de datos de carácter personal. Por su parte Colombia en el año 2011, mediante el Decreto N° 4.886 creó la Delegatura para la Protección de Datos Personales como unidad integrante de la Superintendencia de Industrias y Comercio, cuya función es la regulación de la protección de datos personales, eso sí, dicha unidad no es propiamente una autoridad de control, por cuanto es una unidad o subestructura dependiente de la señalada Superintendencia[560]. También Costa Rica, a través de la Ley N° 8968 de Protección de la Persona, frente al tratamiento de sus datos personales del 5 de noviembre de 2011, en su artículo 15[561] crea a la autoridad de control. Finalmente, España en el año 2013, mediante la Ley de Transparencia y Acceso a la Información Pública creó el Consejo de Transparencia y Buen Gobierno, manteniendo las funciones que desde el año 1994 desempeña la Agencia Española de Protección de Datos.

Finalmente, el cuadro N° 4 también muestra que el ámbito de aplicación y regulación de las autoridades de control en Iberoamérica sobre la protección de datos, abarcan tanto a las instituciones públicas como privadas.

2. Estructura Colegiada o Autoridad Unipersonal – Autónoma o Dependiente

A continuación, se analizará a nivel iberoamericano si la autoridad de control en materia de protección de datos se estructura como un órgano colegiado, cuyo máximo órgano de decisión es una instancia pluripersonal o está dirigida por una única autoridad. De igual forma se describirá si es una agencia o entidad autónoma o independiente, o, por el contrario, depende y está a la tutela o supervigilancia de un organismo superior en la administración del Estado del respectivo país[562].

Cuadro N° 6

PAIS	AUTORIDAD DE CONTROL	COLEGIDA/UNIPERSONAL	DEPENDIENTE/INDEPENDIENTE

53 y 54; II - el 3 de mayo de 2021, con respecto a los otros artículos, esta nueva prórroga se establece por la Medida Provisional N° 959, de 2020).

[560] La Ley 1581/2012 en su Artículo 19 dispone: "Autoridad de Protección de Datos. La Superintendencia de Industria y Comercio, a través de una Delegatura para la Protección de Datos Personales, ejercerá la vigilancia para garantizar que en el Tratamiento de datos personales se respeten los principios, derechos, garantías y procedimientos previstos en la presente ley".

[561] "Créase un órgano de desconcentración máxima adscrito al Ministerio de Justicia y Paz denominado Agencia de Protección de Datos de los habitantes (PRODHAB). Tendrá personalidad jurídica instrumental propia en el desempeño de las funciones que le asigna esta ley, además de la administración de sus recursos y presupuesto, así como para suscribir los contratos y convenios que requiera para el cumplimiento de sus funciones. La Agencia gozará de independencia de criterio"

[562] Estas consideraciones no se analizarán para el Bloque de la Unión Europea, ya que el RGPD establece que la autoridad de control tiene como elemento esencial la independencia, por lo que todos los Estados miembros han adaptado sus estructuras institucionales a las directrices de dicho Reglamento.

Andorra	Agencia Andorrana de Protección de Datos	Unipersonal	Independiente
Argentina	Agencia de Acceso a la Información Pública	Unipersonal	Independiente
Brasil	Autoridad para la Protección de Datos	Colegiada	Independiente
Uruguay	Agencia para el Desarrollo del Gobierno de Gestión Electrónica y la Sociedad de la información y del Conocimiento (AGESIC)	Colegiada[563]	Dependiente[564]
Colombia	Superintendencia de Industria y Comercio	Unipersonal[565]	Independiente

[563] La Unidad Reguladora y de Control de Datos Personales, es una Unidad integrada a la Agencia para el Desarrollo del Gobierno de Gestión Electrónica y la Sociedad de la información y del Conocimiento (AGESIC), que está dirigida por un Consejo que es el Órgano encargado de la dirección técnica y administrativa de la Unidad Reguladora y de Control de Datos Personales, y cuyo cometido sustantivo es "realizar todas las acciones necesarias para el cumplimiento de los objetivos y demás disposiciones de la Ley 18.331, en especial, asistir y asesorar a las personas que lo requieran acerca de los alcances de la ley y el ejercicio de sus derechos; dictar las normas y reglamentaciones; realizar un censo de las bases de datos alcanzados por la ley y mantener el registro permanente de los mismos; controlar la observancia del régimen legal, en particular las normas sobre legalidad, integridad, veracidad, proporcionalidad y seguridad de datos, por parte de los sujetos alcanzados y disponer las actuaciones de fiscalización e inspección pertinentes". Ver sitio web https://www.gub.uy/agencia-gobierno-electronico-sociedad-informacion-conocimiento/institucional/estructura-del-organismo/consejo-ejecutivo-unidad-reguladora-control-datos-personales. consulta efectuada el 19 de junio de 2020.

[564] Según se señala en su propio sitio web https://www.gub.uy/agencia-gobierno-electronico-sociedad-informacion-conocimiento/institucional/estructura-del-organismo/unidad-reguladora-control-datos-personales-0, es: "Órgano de Control creado por la Ley N° 18.331 de Protección de Datos Personales y Acción de Habeas Data (LPDP), con autonomía técnica". Consulta realizada el 19 de junio de 2020.

[565]Como ya se señaló existe una Delegatura de Protección de Datos Personales, cuyas funciones según el Decreto 4886 del año 2011 son: "1. Asesorar al Superintendente de Industria. y Comercio en la formulación de las políticas en lo que se relaciona con su área. 2. Velar por el cumplimiento de las normas y leyes vigentes y proponer nuevas disposiciones. 3. Apoyar a la Oficina de Servicios al Consumidor y de Apoyo Empresarial en el desarrollo de actividades de divulgación, promoción y capacitación, en los temas de su competencia. 4. Disponer el bloqueo temporal de los datos cuando, de la solicitud y de las pruebas aportadas por el Titular, se identifique un riesgo cierto de vulneración de sus derechos fundamentales, y dicho bloqueo sea necesario para protegerlos mientras se adopta una decisión definitiva. 5. Proferir las declaraciones de conformidad sobre las transferencias internacionales de datos. 6. Requerir la colaboración de entidades internacionales o extranjeras cuando se afecten los derechos de los Titulares fuera del territorio colombiano con ocasión, entre otras, de la recolección internacional de datos personales. 7. Decidir los recursos de reposición y las solicitudes de revocatoria directa

Panamá	Autoridad Nacional de Transparencia y Acceso a la Información	Unipersonal	Independiente
Perú	Dirección General de Transparencia, Acceso a la Información Pública y Protección de Datos Personales	Unipersonal	Dependiente[566]
Costa Rica	Agencia de Protección de Datos de los Habitantes	Unipersonal	Dependiente[567]
México	Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos	Colegiada[568]	Independiente
Portugal	Comisión Nacional de Protección de Datos	Colegiada	Independiente
España	Agencia Española de Protección de Datos	Unipersonal	Independiente

Fuente: elaboración propia.

que se interpongan contra los actos que expida, así como los de apelación que se interpongan contra los actos expedidos por la Dirección a su cargo. 8. Dirigir las dependencias a su cargo y velar por el eficiente desempeño de las funciones que les corresponden. 9. Recibir y evaluar los informes que le sean presentados e informar periódicamente al Superintendente sobre el estado de los asuntos de sus dependencias y el grado de ejecución de sus programas. 10. Las demás que le sean asignadas y que correspondan a la naturaleza de la dependencia".

[566] Según se señala en su propio sitio web https://www.minjus.gob.pe/quienes-somos/ : "La Dirección General de Transparencia, Acceso a la Información Pública y Protección de Datos Personales depende jerárquicamente del Despacho Viceministerial de Justicia. Es el órgano de línea encargado de ejercer la Autoridad Nacional de Transparencia y Acceso a la Información Pública, así como de ejercer la Autoridad Nacional de Protección de Datos Personales". Consulta realizada el 19 de junio de 2020.

[567] Según se señala en su propio sitio web http://prodhab.go.cr/quienesomos/: "La Agencia de Protección de Datos de los Habitantes (PRODHAB) es una institución de desconcentración máxima adscrita al Ministerio de Justicia y Paz, con independencia de criterio y personalidad jurídica instrumental propia en el desempeño de sus funciones y en la administración de sus recursos y presupuestos, así como para suscribir los contratos y convenios que requiera para el cumplimiento de sus funciones". Consulta efectuada el 19 de junio de 2020.

[568] El Pleno es el órgano máximo de dirección del INAI y se integra por siete Comisionados designados por el Senado de la República, quienes sesionan periódicamente y cuyas funciones se establecen en la Constitución y en leyes aplicables en la materia promoviendo en todo momento la Transparencia, el Acceso a la información y la Protección de los datos personales.

Como se observa del cuadro precedente, si bien la relación es más estrecha, la mayoría de las entidades de control que regulan y promueven la protección de datos de carácter personal en el bloque iberoamericano se estructuran como organismos unipersonales, en que tienen una única dirección o entidad superior, siendo las autoridades de control de Brasil, México, Portugal y Uruguay dirigidas por una instancia pluripersonal. Además, en el caso de Uruguay, conjuntamente con el Consejo Ejecutivo que dirige la Unidad Reguladora y de Control de Datos Personales, existe un Consejo Consultivo cuyo cometido es asesorar al Consejo Ejecutivo sobre cualquier aspecto de su competencia, debiendo ser consultados por este cuando ejerza potestades de reglamentación, estando integrado por representantes del poder legislativo, judicial, del Ministerio Público, de la academia y del sector privado.

En el caso brasileño la APDP se organiza con una estructura colegiada de dos órganos: el primero la Junta Directiva compuesta por cinco miembros con experiencia en el ámbito de la privacidad y la protección de datos, y el segundo, el Consejo Nacional, que es un comité asesor de 23 miembros con representación del gobierno, la sociedad civil, las instituciones investigadoras y el sector privado.

El modelo español de protección de datos, al igual como ocurre en Alemania, se estructura sobre un órgano unipersonal, a diferencia de otros países europeos que han creado comisiones u órganos colegiados para generar una institucionalidad reguladora de la protección de datos, como es el caso de Francia, Italia y Portugal, los cuales asignan a los directores de sus respectivas agencias la función de velar por el cumplimiento de la legislación sobre protección de datos y controlar su aplicación bajo los estándares del RGPD, garantizando los derechos de las personas en este ámbito, entre los que destacan la resolución de las reclamaciones de las personas contra las Administraciones Públicas por vulneración de los derechos de acceso, rectificación y cancelación; ordenar las inspecciones en los locales o recintos de las Administraciones Públicas donde se encuentren ubicados los ficheros; así como iniciar y resolver motivadamente el procedimiento de infracción a las Administraciones Públicas, entre otras.

Si bien es posible que estas competencias sean mejor desarrolladas a través de órganos colegiados, por cuanto facilita que las decisiones sean compartidas, evitando que la responsabilidad recaiga únicamente sobre una persona, la estructura a través de la cual se configura la Autoridad de Control mucho dependerá de la tradición de cada país en el establecimiento de entidades regulatorias, así como en la idiosincrasia y sesgo cultural con el que funciona la Administración del Estado. Los órganos colegiados favorecen más el debate técnico, la búsqueda de soluciones equilibradas y por consenso que tengan en cuenta los distintos intereses en juego. Pero a su vez pueden ralentizar las decisiones y generar más espacio para la burocracia interna, diluyendo las responsabilidades y desincentivado la rendición de cuentas.

En relación a la autonomía o independencia de la autoridad de control, se observa que 5 de las agencias encargadas de la protección de datos tienen independencia en el desempeño de sus funciones, versus las entidades de Uruguay, Perú y Costa Rica, cuyas autoridades de control dependen de otros organismos, eso sí conviene precisar que la entidad uruguaya goza de autonomía técnica en el desempeño de sus funciones, a diferencia de las instituciones peruana y costarricense encargadas de la protección de datos, que dependen del Ministerio de Justicia y del Ministerio de Justicia y Paz respectivamente, modelo que no cumpliría con los estándares

establecidos por el RGPD que recomienda independencia del poder político, siendo los ministerios entidades que precisamente tienen dicho carácter[569].

Consideraciones sobre la Autoridad de Control en la Experiencia Comparada

De la revisión realizada a la configuración de las autoridades de control en Europa, en la OCDE e Iberoamérica, si bien es difícil establecer un patrón común en su forma de estructuración, es posible colegir algunas consideraciones iniciales, las que deben ser complementadas por diversos factores, tales como idiosincrasia, sistema jurídico (romanista o common law), régimen de gobierno, aspectos demográficos e incluso económicos. Estas consideraciones preliminares son:

a) Evidentemente son mayoritarios los modelos únicos en que la autoridad de control se estructura exclusivamente para regular la protección de datos de carácter personal.

b) La fecha de creación de las agencias de control en la experiencia comparada también es muy amplia y diversa, por ejemplo, Portugal crea su institucionalidad en 1978 y Japón hace lo propio en el año 2016. En el caso latinoamericano Brasil crea su Agencia de Protección de Datos en el año 2018, que entrará en plenas funciones en el año 2021.

c) Si bien los modelos únicos son mayoritarios, países que ejercen una importante influencia, tanto económica y también política en sus respectivos bloques, han optado por sistemas mixtos, donde las autoridades de control regulan simultáneamente la protección de datos y el acceso a la información pública. Tal es el caso de Alemania y Reino Unido en Europa y México y Argentina en Latinoamérica.

d) En la mayoría de los países en que existe un sistema mixto, las entidades o agencias de control primero han regulado exclusivamente la protección de datos personales y luego, a través de reformas institucionales, han asumido la función de tutelar también el derecho de acceso a la información pública. Ese es el caso por ejemplo de Australia con la *Office of the Australian Information Comissioner OAIC,* cuya ley de 1998 le asignó competencias en materia de protección de datos personales y luego en el año 2010 se le asignaron funciones en materia de derecho de acceso a la información pública. Los mismo ocurre con el Reino Unido, ya que la *Information Commissioner´s Office ICO,* asume la protección de datos personales en el año 1998 con la *Data Protection Act,* la que es modificada en el año 2004 por la *Freedom of Infromation Act and data protection Act* asumiendo el sistema mixto. A nivel

[569] A nivel latinoamericano como se analizó en el capitulo III de esta investigación, la autoridad de control de Nicaragua en materia de protección de datos también depende del Ministerio de Hacienda de dicho país.

latinoamericano ocurre algo similar[570], Argentina primero crea la Dirección Nacional de Protección de Datos reglamentada por el Decreto N° 1558, del año 2001, y luego en el año 2016, mediante la Ley N° 27.275 crea la Agencia de Acceso a la Información Pública que se configura en un sistema mixto. Así también ocurre en Perú, que primero crea la Dirección de Protección de Datos y luego la Dirección de Transparencia y Acceso a la Información, adscribiendo ambas al Ministerio de Justicia-Dirección General de Transparencia, Acceso a la información y Protección de Datos.

e) En el contexto Iberoamericano, la mayoría (7) de las agencias encargadas de la protección de datos se estructuran con una autoridad de control unipersonal, que es también el modelo que mayoritariamente siguen las agencias de los Estados miembros de la UE.

f) Si bien en Europa y también en la OCDE la mayoría de las autoridades de control tienen independencia y altos niveles de autonomía en el ejercicio de sus funciones y poderes (en la UE la independencia de la autoridad de control es un requisito esencial), en el caso iberoamericano hay algunas agencias, como las de Perú y Costa Rica, que dependen de la autoridad política (de los ministerios) para la regulación de la protección de datos de carácter personal.

La Autoridad de Control en España

Como se ha podido observar en el desarrollo de este trabajo, el RGPD fortalece a las autoridades de control, tanto en sus funciones como en la posibilidad de imponer sanciones, de manera que puedan ser efectivas en la supervisión y aplicación de la protección de datos, unificando su capacidad coercitiva estableciendo mecanismos que faciliten la coherencia en la aplicación de la protección de datos en toda la Unión. El Reglamento supone, de alguna manera, un reconocimiento implícito del modelo español de protección de datos personales y de la actividad de supervisión y control que ha desempeñado la Agencia Española de Protección de Datos en las últimas dos décadas.

En las siguientes líneas se revisarán los orígenes, funciones y estructura que la Agencia Española asume, con la nueva regulación reglamentaria.

Como ya se ha señalado, la Constitución Española de 1978 prevé en su artículo 18.4 que el legislador limitará el uso de la informática para proteger los derechos fundamentales de los ciudadanos, de igual forma el Tribunal Constitucional estableció en su Sentencia N° 292/2000 que el derecho a la protección de datos es un derecho fundamental, autónomo y claramente diferenciado de los demás que se garantizan en el mismo artículo 18 de la CE. Dicha sentencia establece que este derecho: “persigue garantizar a esa persona un poder de control sobre sus

[570] La excepción la representa México mediante el Instituto Nacional de Acceso a la Información y Protección de Datos, que primero abordó el acceso a la información pública y luego la protección de datos de carácter personal.

datos personales, sobre su uso y destino, con el propósito de impedir su tráfico ilícito y lesivo para la dignidad y derecho del afectado".

La existencia de una autoridad independiente que vele por este derecho está prevista en el Convenio 108 del Consejo de Europa del año 1981, el primer texto internacional sobre la materia, que seguía el criterio organizativo y funcional de atribuir a una autoridad independiente la función de velar por el cumplimiento de la normativa de protección de datos. Este criterio, que establece la existencia de una autoridad independiente, se acaba convirtiendo en el modelo europeo, sobre la base de diversos textos que así lo establecen: la Carta Europea de Derechos Fundamentales, la Directiva 95/46/CE, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de esos datos, y finalmente en Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016, sobre la protección de las personas físicas en lo que concerniente al tratamiento de datos personales y a la libre circulación de estos datos.

Siguiendo los lineamentos del RGPD y los que ya establecía la Directiva 95/46/CE, la Agencia Española de Protección de Datos (AEPD) es una entidad de naturaleza independiente, con presupuesto propio y plena autonomía funcional[571].

La AEPD se creó en 1992 y comenzó a funcionar en el año 1994. En efecto, la Ley Orgánica 5/1992 del 29 de octubre, que regula el tratamiento automatizado de datos de carácter personal, en su Título VI crea la Agencia de Protección de Datos como una entidad independiente que debe garantizar el cumplimiento de lo previsto en dicha ley, estando reguladas algunas de sus funciones y tareas en ese precepto legal, como también en el Real Decreto 428/1993, de 26 de marzo, por el que se aprueba el Estatuto de la Agencia de Protección de Datos[572], el que

[571] De la web de la Agencias Española de Protección de Datos; www.aepd.es, es posible extraer que "La Agencia Española de Protección de Datos es una autoridad administrativa independiente de ámbito estatal, de las previstas en la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del sector Público, con personalidad jurídica y plena capacidad pública y privada, que actúa con plena independencia de los poderes públicos en el ejercicio de sus funciones. Constituye la "autoridad de control" que el Reglamento General de Protección de Datos determina que establecerán los Estados miembros a efectos de supervisar su aplicación, con el fin de proteger los derechos y las libertades fundamentales de las personas físicas en lo que respecta al tratamiento y de facilitar la libre circulación de datos personales en la Unión. La Presidencia de la Agencia y su Adjunto serán nombrados por el Gobierno, a propuesta del Ministerio de Justicia, entre personas de reconocida competencia profesional, en particular en materia de protección de datos".

[572] Estos Estatutos se referían a la naturaleza y régimen jurídico de la AEPD, en sus artículo primero y segundo*;* "Artículo 1. La Agencia de Protección de Datos. 1. La Agencia de Protección de Datos es un ente de Derecho público de los previstos en el artículo 6, apartado 5, del texto refundido de la Ley General Presupuestaria, aprobado por Real Decreto legislativo 1091/1988, de 23 de septiembre, que tiene por objeto la garantía del cumplimiento y aplicación de las previsiones contenidas en la Ley Orgánica 5/1992, de 29 de octubre, de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal.

2. La Agencia de Protección de Datos actúa con plena independencia de las Administraciones Públicas en el ejercicio de sus funciones y se relaciona con el Gobierno a través del Ministerio de Justicia.

Artículo 2. Régimen jurídico.1. La Agencia de Protección de Datos goza de personalidad jurídica propia y plena capacidad pública y privada. 2. La Agencia de Protección de Datos se regirá por las disposiciones legales y reglamentarias siguientes: a) El título VI de la Ley Orgánica 5/1992, de 29 de octubre, de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal. b) El presente Estatuto y las demás disposiciones

continua vigente en todo lo que no contravenga la legislación actual. Esa legislación actual, es la Ley Orgánica 3/2018 de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales[573], LOPDGDD, que surge como adaptación de la legislación española al Reglamento General Europeo. Esta ley, en su Título VII sobre Autoridades de protección de datos, en el capítulo primero, sección primera sobre disposiciones generales, se refiere a la Agencia Española de Protección de Datos, al disponer en su artículo 44:

> *"1. La Agencia Española de Protección de Datos es una autoridad administrativa independiente de ámbito estatal, de las previstas en la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, con personalidad jurídica y plena capacidad pública y privada, que actúa con plena independencia de los poderes públicos en el ejercicio de sus funciones. Su denominación oficial, de conformidad con lo establecido en el artículo 109.3 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, será "Agencia Española de Protección de Datos, Autoridad Administrativa Independiente". Se relaciona con el Gobierno a través del Ministerio de Justicia. 2. La Agencia Española de Protección de Datos tendrá la condición de representante común de las autoridades de protección de datos del Reino de España en el Comité Europeo de Protección de Datos. 3. La Agencia Española de Protección de Datos y el Consejo General del Poder Judicial colaborarán en aras del adecuado ejercicio de las*

de desarrollo de la Ley Orgánica 5/1992. c) En defecto de las anteriores, y para el ejercicio de sus funciones públicas, las normas de procedimiento contenidas en la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común. d) Los preceptos de la Ley General Presupuestaria, texto refundido aprobado por Real Decreto legislativo 1091/1988, de 23 de septiembre, que resulten de aplicación. e) Cuantas otras disposiciones resulten de aplicación. 3. La Agencia ejercerá sus funciones por medio del Director, a cuyo efecto los actos del Director se consideran actos de la Agencia. 4. Los actos dictados por el Director en el ejercicio de las funciones públicas de la Agencia agotan la vía administrativa. Contra ellos se podrán interponer los recursos contencioso-administrativos que resulten procedentes".

[573]La cronología de la Ley Orgánica de Protección de Datos Personales y Garantía de Derechos Digitales es la siguiente: El 19 de mayo de 2017 se aprueba el borrador por la Comisión General de Codificación (Sección de Derecho Público). También en el año 2017, el 23 de junio se aprueba Anteproyecto de Ley Orgánica de Protección de Datos de carácter personal; el 11 de julio se evacua el Informe de la Agencia Española de Protección de Datos; el 14 de julio Informe del Consejo Fiscal; el 14 de agosto Informe del Consejo General del Poder Judicial; el 26 de octubre Dictamen del Consejo de Estado; el 10 de noviembre el Consejo de Ministros aprueba la remisión a las Cortes Generales del Proyecto de Ley Orgánica de Protección de Datos para adaptar la legislación española al RGPD; el 24 de noviembre Iniciativa, Boletín oficial de las Cortes Generales, Congreso de los Diputados n° A-13-1. En el año 2018, el 18 de abril, enmiendas e índice de enmiendas al articulado, Boletín oficial de las Cortes Generales. Congreso de los Diputados n° A-13-2; el 9 de octubre, Informe de la Ponencia, Boletín oficial de las Cortes Generales. Congreso de los Diputados n° A-13-3; el 17 de octubre Dictamen de la Comisión, Boletín oficial de las Cortes Generales. Congreso de los Diputados n° A-13-4; 23 de octubre, Texto remitido por el Congreso de los Diputados, Boletín oficial de las Cortes Generales. Senado n° 289; 24 de octubre, Escrito de mantenimiento de enmiendas para su defensa ante el pleno. Boletín oficial de las Cortes Generales. Congreso de los Diputados n° A-13-5; 26 de octubre, Aprobación por el Pleno, Boletín oficial de las Cortes Generales. Congreso de los Diputados n° A-13-6; 14 de noviembre, Enmiendas Senado. Boletín oficial de las Cortes Generales. Senado n° 298; 15 de noviembre, Índice de enmiendas, Boletín oficial de las Cortes Generales. Senado n° 299; 20 de noviembre, Informe de Ponencias, Senado. Boletín oficial de las Cortes Generales. Senado n° 302; 20 de noviembre Dictamen de la Comisión, Senado. Boletín oficial de las Cortes Generales. Senado n° 302; 26 de noviembre, Texto aprobado por el Senado. Boletín oficial de las Cortes Generales. Senado n° 306; Publicación de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de datos Personales y garantía de los derechos digitales. BOE n° 294, de 6 de diciembre de 2018.

> *respectivas competencias que la Ley Orgánica 6/1985, de 1 julio, del Poder Judicial, les atribuye en materia de protección de datos personales en el ámbito de la Administración de Justicia"*.

Es importante precisar que la Ley 40/2015, establece el Régimen Jurídico del Sector Público Estatal, que se aplica a la Administración General del Estado, a la Administración de las Autoridades Autonómicas y de la Administración Local, así como a lo que se denomina sector público institucional. La organización y funcionamiento de este último sector está integrado entre otras por las autoridades administrativas independientes, las que en el ámbito estatal son aquellas entidades de derecho público que vinculadas a la estructura de la Administración del Estado, tienen personalidad jurídica propia y gozan de funciones de regulación de carácter externo sobre determinados sectores o actividades económicas, las que requieren una especial autonomía de la Administración General del Estado, la que deberá ser establecida por ley. Tales entidades deberán singularizarse en su denominación como autoridades administrativas independientes, "A.A.I", tal como lo indica el artículo 44 de la Ley 3/2018, al definir a la AEPD.

En relación con el apartado dos del artículo 44, este reconoce implícitamente la existencia en España de otras autoridades de control, que precisamente son las de las tres autoridades autonómicas (Autoridad Vasca, Autoridad Catalana de Protección de Datos, así como el Consejo para la Transparencia y Protección de Datos de Andalucía). Disponiendo que la AEPD es la representante ante el Comité Europeo de Protección de Datos.

Luego, el artículo 45 de la ley, a propósito del régimen jurídico de la AEPD, señala que;

> *"1. La Agencia Española de Protección de Datos se rige por lo dispuesto en el Reglamento (UE) 2016/679, la presente ley orgánica y sus disposiciones de desarrollo. Supletoriamente, en cuanto sea compatible con su plena independencia y sin perjuicio de lo previsto en el artículo 63.2 de esta ley orgánica, se regirá por las normas citadas en el artículo 110.1 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público. 2. El Gobierno, a propuesta de la Agencia Española de Protección de Datos, aprobará su Estatuto mediante real decreto"*.

Por su parte, el artículo 46 de la LOPDPGDD se refiere al régimen económico, presupuestario y de personal de la Agencia, ya que como es lógico es una garantía de independencia que la Agencia esté dotada de los recursos tanto económicos, materiales y humanos, que le permitan desempeñar sus funciones y ejercer sus poderes.

> *Artículo 46 de la LOPDPGDD; "Régimen económico presupuestario y de personal. 1. La Agencia Española de Protección de Datos elaborará y aprobará su presupuesto y lo remitirá al Gobierno para que sea integrado, con independencia, en los Presupuestos Generales del Estado. 2. El régimen de modificaciones y de vinculación de los créditos de su presupuesto será el establecido en el Estatuto de la Agencia Española de Protección de Datos. Corresponde a la Presidencia de la Agencia Española de Protección de Datos autorizar las modificaciones presupuestarias que impliquen hasta un tres por ciento de la cifra inicial de su presupuesto total de gastos,*

> *siempre que no se incrementen los créditos para gastos de personal. Las restantes modificaciones que no excedan de un cinco por ciento del presupuesto serán autorizadas por el Ministerio de Hacienda y, en los demás casos, por el Gobierno. 3. La Agencia Española de Protección de Datos contará para el cumplimiento de sus fines con las asignaciones que se establezcan con cargo a los Presupuestos Generales del Estado, los bienes y valores que constituyan su patrimonio y los ingresos, ordinarios y extraordinarios derivados del ejercicio de sus actividades, incluidos los derivados del ejercicio de las potestades establecidos en el artículo 58 del Reglamento (UE) 2016/679. 4. El resultado positivo de sus ingresos se destinará por la Agencia Española de Protección de Datos a la dotación de sus reservas con el fin de garantizar su plena independencia. 5. El personal al servicio de la Agencia Española de Protección de Datos será funcionario o laboral y se regirá por lo previsto en el texto refundido de la Ley del Estatuto Básico del Empleado Público, aprobado por Real Decreto Legislativo 5/2015, de 30 de octubre, y demás normativa reguladora de los funcionarios públicos y, en su caso, por la normativa laboral. 6. La Agencia Española de Protección Datos elaborará y aprobará su relación de puestos de trabajo, en el marco de los criterios establecidos por el Ministerio de Hacienda, respetando el límite de gasto de personal establecido en el presupuesto. En dicha relación de puestos de trabajo constarán, en todo caso, aquellos puestos que deban ser desempeñados en exclusiva por funcionarios públicos, por consistir en el ejercicio de las funciones que impliquen la participación directa o indirecta en el ejercicio de potestades públicas y la salvaguarda de los intereses generales del Estado y de las Administraciones Públicas. 7. Sin perjuicio de las competencias atribuidas al Tribunal de Cuentas, la gestión económico-financiera de la Agencia Española de Protección de Datos estará sometida al control de la Intervención General de la Administración del Estado en los términos que establece la Ley 47/2003, de 26 de noviembre, General Presupuestaria."*

En este sentido, y siguiendo también las directrices del RGPD, la Agencia Española de Protección de Datos elabora y aprueba su presupuesto, remitiéndolo al Gobierno para que sea integrado con independencia en los presupuestos generales del Estado. Además de las asignaciones establecidas con cargo a dichos presupuestos la AEPD cuenta con sus propios ingresos ordinarios y extraordinarios generados por el ejercicio de sus facultades sancionadoras. El resultado de tales ingresos se destina a la dotación de reservas de la Agencia, lo que también contribuye a asegurar su independencia.

De igual forma la AEPD selecciona directamente a su personal, siendo sus funcionarios regulados por el Estatuto Básico del Empleado Público, aprobado mediante el Real Decreto Legislativo 5/2015, de 30 de octubre. Es la propia Agencia la que propone al Ministerio de Hacienda y Función Pública la dotación de su personal, lo que representa un cambio en la materia, ya que, hasta antes de la LOPDGDD, esta propuesta de puestos de trabajo era enviada a través del Ministerio de Justicia, según se dispone en los Estatutos de la AEPD, con esta comunicación directa al Ministerio de Hacienda, se fortalece el carácter autónomo e independiente de la misma.

Así lo señala también Manuel Sanchez de Diego Fernandez de la Riva en contraste con el Consejo para la Transparencia y Buen Gobierno (CTBG); "La autonomía financiera implica el

control de sus recursos económicos, tanto de los propios como de los públicos. En este sentido, no solo el CTBG, también los otros órganos autonómicos garantes de la trasparencia han señalado en la Declaración de Cádiz (2018) los obstáculos y retos a los que se enfrentan, como es *"la falta de recursos económicos y, en su consecuencia, materiales y personales de los Consejos y Comisionados de Transparencia; la situación de debilidad de las Administraciones y organismos públicos de menor tamaño y reducida estructura, que se enfrentan a dificultades organizativas y de toda índole, para atender eficazmente las obligaciones derivadas de las políticas de transparencia"*. Este problema de medios se reitera en la Declaración de Málaga (2019) cuando se demanda *"La exigencia de garantizar el reconocimiento y el adecuado apoyo material a los Consejos y Comisiones de Transparencia, a nivel nacional y a nivel autonómico"*. A diferencia de la Agencia Española de Protección de Datos Personales que genera una importante recaudación por las multas impuestas por infracciones en la protección de datos personales, el CTBG carece de potestad sancionadora"[574].

La independencia de la Agencia también se expresa en la posibilidad de adherir a los sistemas de contratación centralizada establecidos por las Administraciones Públicas y participar en la gestión compartida de servicios comunes prevista en el artículo 85 de la Ley 40/2015, sobre Régimen Jurídico del Sector Público, lo que permite que la AEPD se acoja al sistema de contratación centralizada o licite directamente, lo que flexibiliza su gestión.

La independencia jurídica y económica de la Autoridad de Control no significa que no esté afecta a la verificación o supervisión de sus actuaciones, por lo que, sin perjuicio de la intervención del Tribunal de Cuentas, la gestión económica financiera de la Agencia está sometida al control de la Intervención General de la Administración del Estado, según lo dispone la Ley 47/2003, de 26 de noviembre, General Presupuestaria.

El artículo 47 de la LOPDGDD se refiere a las funciones y potestades de la Agencia Española de Protección de Datos, señalando que para supervisar la aplicación de esta y del RGPD, además de ejercer las funciones establecidas en el artículo 57 y las potestades previstas en el artículo 58 del mismo Reglamento, le corresponde a la Agencia Española de Protección de Datos el desempeño de las funciones y potestades que le atribuyan otras leyes o normas de Derecho de la Unión Europea.

Finalmente, en lo relativo a la estructura y organización de la AEPD, los artículos 48 y 49 de la LOPDGDD se refieren respectivamente a la Presidencia y al Consejo Consultivo de la Agencia.

> *Artículo 48 de la LOPDGDD; "La Presidencia de la Agencia Española de Protección de Datos. 1. La Presidencia de la Agencia Española de Protección de Datos la dirige, ostenta su representación y dicta sus resoluciones, circulares y directrices. 2. La Presidencia de la Agencia Española de Protección de Datos estará auxiliada por un Adjunto en el que podrá delegar sus funciones, a excepción de las relacionadas con*

[574] Sánchez de Diego Fernández de la Riva, M. (2022) *El derecho de acceso a la información. Un tortuoso camino*. Colección Fragua Comunicación nº 207. Madrid. Editorial Fragua, pp. 366-367.

los procedimientos regulados por el Título VIII de esta ley orgánica, y que la sustituirá en el ejercicio de las mismas en los términos previstos en el Estatuto Orgánico de la Agencia Española de Protección de Datos. Ambos ejercerán sus funciones con plena independencia y objetividad y no estarán sujetos a instrucción alguna en su desempeño. Les será aplicable la legislación reguladora del ejercicio del alto cargo de la Administración General del Estado. 3. La Presidencia de la Agencia Española de Protección de Datos y su Adjunto serán nombrados por el Gobierno, a propuesta del Ministerio de Justicia, entre personas de reconocida competencia profesional, en particular en materia de protección de datos. Dos meses antes de producirse la expiración del mandato o, en el resto de las causas de cese, cuando se haya producido éste, el Ministerio de Justicia ordenará la publicación en el Boletín Oficial del Estado de la convocatoria pública de candidatos. Previa evaluación del mérito, capacidad, competencia e idoneidad de los candidatos, el Gobierno remitirá al Congreso de los Diputados una propuesta de Presidencia y Adjunto acompañada de un informe justificativo que, tras la celebración de la preceptiva audiencia de los candidatos, deberá ser ratificada por la Comisión de Justicia en votación pública por mayoría de tres quintos de sus miembros en primera votación o, de no alcanzarse ésta, por mayoría absoluta en segunda votación, que se realizará inmediatamente después de la primera. En este último supuesto, los votos favorables deberán proceder de Diputados pertenecientes, al menos, a dos grupos parlamentarios diferentes. 4. La Presidencia y el Adjunto de la Agencia Española de Protección de Datos serán nombrados por el Consejo de Ministros mediante real decreto. 5. El mandato de la Presidencia y del Adjunto de la Agencia Española de Protección de Datos tiene una duración de cinco años y puede ser renovado para otro período de igual duración. La Presidencia y el Adjunto solo cesarán antes de la expiración de su mandato, a petición propia o por separación acordada por el Consejo de Ministros, por: a) Incumplimiento grave de sus obligaciones, b) incapacidad sobrevenida para el ejercicio de su función, c) incompatibilidad, o d) condena firme por delito doloso. En los supuestos previstos en las letras a), b) y c) será necesaria la ratificación de la separación por las mayorías parlamentarias previstas en el apartado 3 de este artículo. 6. Los actos y disposiciones dictados por la Presidencia de la Agencia Española de Protección de Datos ponen fin a la vía administrativa, siendo recurribles, directamente, ante la Sala de lo Contencioso-administrativo de la Audiencia Nacional".

Artículo 49 de la LOPDGDD; "Consejo Consultivo de la Agencia Española de Protección de Datos. 1. La Presidencia de la Agencia Española de Protección de Datos estará asesorada por un Consejo Consultivo compuesto por los siguientes miembros: a) Un Diputado, propuesto por el Congreso de los Diputados. b) Un Senador, propuesto por el Senado. c) Un representante designado por el Consejo General del Poder Judicial. d) Un representante de la Administración General del Estado con experiencia en la materia, propuesto por el Ministro de Justicia. e) Un representante de cada Comunidad Autónoma que haya creado una Autoridad de protección de datos en su ámbito territorial, propuesto de acuerdo con lo que establezca la respectiva Comunidad Autónoma. f) Un experto propuesto por la Federación Española de Municipios y Provincias. g) Un experto propuesto por el Consejo de Consumidores y Usuarios. h) Dos expertos propuestos por las

Organizaciones Empresariales. i) Un representante de los profesionales de la protección de datos y de la privacidad, propuesto por la asociación de ámbito estatal con mayor número de asociados. j) Un representante de los organismos o entidades de supervisión y resolución extrajudicial de conflictos previstos en el Capítulo IV del Título V, propuesto por el Ministro de Justicia. k) Un experto, propuesto por la Conferencia de Rectores de las Universidades Españolas. l) Un representante de las organizaciones que agrupan a los Consejos Generales, Superiores y Colegios Profesionales de ámbito estatal de las diferentes profesiones colegiadas, propuesto por el Ministro de Justicia. m) Un representante de los profesionales de la seguridad de la información, propuesto por la asociación de ámbito estatal con mayor número de asociados. n) Un experto en transparencia y acceso a la información pública propuesto por el Consejo de Transparencia y Buen Gobierno. ñ) Dos expertos propuestos por las organizaciones sindicales más representativas. 2. A los efectos del apartado anterior, la condición de experto requerirá acreditar conocimientos especializados en el Derecho y la práctica en materia de protección de datos mediante el ejercicio profesional o académico. 3. Los miembros del Consejo Consultivo serán nombrados por orden del Ministro de Justicia, publicada en el Boletín Oficial del Estado. 4. El Consejo Consultivo se reunirá cuando así lo disponga la Presidencia de la Agencia Española de Protección de Datos y, en todo caso, una vez al semestre. 5. Las decisiones tomadas por el Consejo Consultivo no tendrán en ningún caso carácter vinculante. 6. En todo lo no previsto por esta ley orgánica, el régimen, competencias y funcionamiento del Consejo Consultivo serán los establecidos en el Estatuto Orgánico de la Agencia Española de Protección de Datos".

Sobre este punto es importante precisar que esta reformulación en la estructura organizacional de la Agencia, establecida en la Ley 3/2018, aún no se concreta, manteniéndose vigente lo dispuesto en la Ley Orgánica de Protección de datos – LOPD, Ley 15/1999, de 13 de diciembre[575], a la espera del nuevo Estatuto de esta, por cuanto el vigente, contenido como ya se señaló en el Real Decreto 428/1993, de 26 de marzo, dispone también, al igual que la LOPD, la existencia de un Director[576].

[575] En su artículo 36 se refiere al Director de la Agencia Española de Protección de Datos, estableciendo; "El Director. 1. El Director de la Agencia de Protección de Datos dirige la Agencia y ostenta su representación. Será nombrado, de entre quienes componen el Consejo Consultivo, mediante Real Decreto, por un período de cuatro años. 2. Ejercerá sus funciones con plena independencia y objetividad y no estará sujeto a instrucción alguna en el desempeño de aquéllas. En todo caso, el Director deberá oír al Consejo Consultivo en aquellas propuestas que éste le realice en el ejercicio de sus funciones. 3. El Director de la Agencia de Protección de Datos sólo cesará antes de la expiración del período a que se refiere el apartado 1, a petición propia o por separación acordada por el Gobierno, previa instrucción de expediente, en el que necesariamente serán oídos los restantes miembros del Consejo Consultivo, por incumplimiento grave de sus obligaciones, incapacidad sobrevenida para el ejercicio de su función, incompatibilidad o condena por delito doloso. 4. El Director de la Agencia de Protección de Datos tendrá la consideración de alto cargo y quedará en la situación de servicios especiales si con anterioridad estuviera desempeñando una función pública. En el supuesto de que sea nombrado para el cargo algún miembro de la carrera judicial o fiscal pasará asimismo a la situación administrativa de servicios especiales".

[576] En efecto el artículo 11 del Estatuto se refiere a Estructura orgánica. "La Agencia de Protección de Datos se estructura en los siguientes órganos: 1. El Director de la Agencia de Protección de Datos. 2. El Consejo

La nueva ley cambia la denominación del titular de la Agencia, pasando a ser una Presidencia en vez de una Dirección, la que además será asistida por un Adjunto, esta última figura, la de Adjunto, si bien existía en la normativa anterior, no tenía ni la jerarquía ni las funciones que ahora le asigna la LOPDGDD. La Presidencia se encuentra habilitada para dictar resoluciones, circulares y directrices, que son las mismas facultades que podrá ejercer el Adjunto vía delegación administrativa, a excepción de las facultades relacionadas con la investigación y sustanciación de procedimientos administrativos sancionatorios.

Es importante precisar, a propósito de la delegación administrativa, que esta implica un acto en que se delega el ejercicio de las atribuciones, no las facultades mismas, que siguen radicadas en la Presidencia de la Agencia [577].

El nombramiento del Presidente y del Adjunto es propuesto por el Ministro de Justicia, realizándolo el Consejo de Ministros mediante Real Decreto, previo a ello se debe desarrollar un procedimiento que debe desplegarse con mayor detalle en el respectivo Estatuto de la AEPD, donde los candidatos deben acreditar una trayectoria y experiencia reconocida en materia de protección de datos de carácter personal.

La Ley 3/2018 establece también que entre un Presidente de la Agencia y la asunción de su sucesor[578], dos meses antes de producirse la expiración del mandato o cuando esta se produjera por diversas circunstancias, el Ministro de Justicia ordenará la publicación en el Boletín Oficial del Estado BOE, convocando públicamente a postular.

Conocidos los candidatos, se realizará una evaluación de sus capacidades, competencias y méritos, que luego el Gobierno remitirá al Congreso de los Diputados, con una propuesta para la Presidencia y para el Adjunto, acompañada de un informe que sustente la selección. A continuación, la Comisión de Justicia del Congreso de los Diputados recibirá en audiencia a

---

Consultivo. 3. El Registro General de Protección de Datos, la Inspección de Datos y la Secretaría General, como órganos jerárquicamente dependientes del Director de la Agencia".

[577] La Delegación a la que se hace referencia es la misma que está regulada en el ordenamiento jurídico chileno, en el artículo 41 de la Ley Orgánica Constitucional de Bases Generales de la Administración del Estado N° 18.575, que dispone; "El ejercicio de las atribuciones y facultades propias podrá ser delegado, sobre las bases siguientes: a) La delegación deberá ser parcial y recaer en materias específicas; b) Los delegados deberán ser funcionarios de la dependencia de los delegantes; c) El acto de delegación deberá ser publicado o notificado según corresponda; d) La responsabilidad por las decisiones administrativas que se adopten o por las actuaciones que se ejecuten recaerá en el delegado, sin perjuicio de la responsabilidad del delegante por negligencia en el cumplimiento de sus obligaciones de dirección o fiscalización; y e) La delegación será esencialmente revocable. El delegante no podrá ejercer la competencia delegada sin que previamente revoque la delegación. Podrá igualmente, delegarse la facultad de firmar, por orden de la autoridad delegante, en determinados actos sobre materias específicas. Esta delegación no modifica la responsabilidad de la autoridad correspondiente, sin perjuicio de la que pudiera afectar al delegado por negligencia en el ejercicio de la facultad delegada".

[578] Su periodo de mandato dura 5 años, pudiendo renovarse por igual periodo. En la actualidad el mandato del Director de la AEPD se extiende por 4 años. En el año 2022 por primera vez se seguirá el nuevo sistema de designación. Desde la sociedad civil se ha reclamado que los curricula vitae de los candidatos se publiquen antes de su designación. Véase Blanes, Miguel Ángel(2021): *La falta de transparencia del proceso selectivo para la designación de la Presidencia de la Agencia Española de Protección de Datos* https://miguelangelblanes.com/2021/12/27/la-falta-de-transparencia-del-proceso-selectivo-para-la-designacion-de-la-presidencia-de-la-agencia-espanola-de-proteccion-de-datos/

los postulantes y luego ratificarán la selección propuesta por el Ministerio de Justicia, en votación pública por las 3/5 partes de sus integrantes en primera votación, o de no alcanzarse dicho quórum por la mayoría absoluta de sus miembros en segunda votación. En el caso de tener que realizar esta segunda votación, que es inmediatamente después de la primera, los votos deberán ser a lo menos de dos grupos parlamentarios diferentes.

En lo que respecta al Consejo Consultivo de la Agencia, la LOPDGDD también presenta novedades, por cuanto incorpora a nuevos actores, como los profesionales ligados a la protección de datos y a la privacidad o a los profesionales de la seguridad de la información. Además, se suma al Consejo un representante de las entidades de supervisión y resolución extrajudicial de conflictos que ejercerán un relevante rol como órgano de control de cumplimiento de los códigos de conducta. También se integra el representante del Consejo de Transparencia y Buen Gobierno, entidad que se crea en el año 2013[579], lo que mejorará las interacciones evidentes que en muchas ocasiones existirán entre la protección de datos y el acceso a la información pública.

Por último, se incorporan al Consejo dos expertos propuestos por las organizaciones sindicales más representativas. "La Agencia siempre ha pretendido la participación de los agentes sociales en aquellas tomas de decisión de protección de datos que podrían afectar a los trabajadores. En el año 2008, en la tramitación de autorizaciones internacionales de datos se incluyó un trámite de información pública para que pudiesen realizar alegaciones. Este paso tenía razón de ser debido a la posible consecuencia que podría tener una autorización de transferencias internacionales de datos de la deslocalización de puestos de trabajo" [580].

Consideraciones Finales

Como ya se señaló, el Reglamento [Europeo] General de Protección de Datos, establece como un elemento fundamental de las autoridades de control su carácter autónomo o independiente. Dicho carácter no es solo una autonomía al ejecutivo o gobierno, sino también una independencia de los poderes políticos del Estado, evitando así una eventual captura de las fuerzas políticas sobre la Administración. El estándar, entonces, para las entidades que ejercen funciones de control, es lo que algunos autores han denominado una "neutralidad amplia", sacando en este caso, la regulación y promoción de la protección de datos de carácter personal, de las decisiones que pudieran ser fluctuantes dependiendo de la influencia que determinadas fuerzas políticas ejerzan en momentos también determinados[581].

---

[579] La Ley 19/2013, de 9 de noviembre sobre Transparencia, Acceso a la Información Pública y Buen Gobierno incorpora también ha dicho Consejo a un representante de la AEPD.

[580] Blanco Antón, M. J. (2019), "Autoridades de Control Independientes (Arts. 51-59 RGPD). Autoridades de Protección de Datos (Arts. 44-59 y Disposición adicional cuarta LOPDGDD)", en "*La Adaptación al Nuevo Marco de Protección de Datos tras el RGPD y la LOPDGDD"*, Coordinador José López Calvo, Boch Wolters Kluwer, p. 617.

[581] Por ejemplo, para Karl Loewenstein, el objetivo de las autoridades independientes es librar a la administración del control del gobierno, de los partidos y también del parlamento; en Loewenstein, K. (1986), "*Teoría de la Constitución"*, 2º ed. Ariel, Barcelona, p. 439; también, García, E. de Enterría y Fernández, T. R. (2020), "*Curso*

La independencia de las entidades de control encuentra también su sustento en las funciones de supervisión, regulación y sanción que deben ejercer. En efecto, la independencia tiene su causal o motivo en que dichas funciones son eminentemente jurídicas y no políticas, por lo que cuando una entidad de la administración lleva a cabo una actividad de regulación, esta no debe efectuarse atendiendo a criterios políticos sino exclusivamente técnicos. Además, el ejercicio de esas funciones no es el ejercicio de la soberanía, que indisolublemente es una actividad política radicada en el pueblo.

La soberanía y su ejercicio constituye una actividad decisoria que conlleva la elección o preferencia de determinados fines o propósitos por sobre otros, que componen intereses y que es aplicación, en muchos casos, de una ideología determinada.

Toda decisión política es una decisión soberana. Por ello, esta decisión soberana debe de ser reconducible al titular de la soberanía, que es el Pueblo, ya sea directamente o a través de sus representantes. La democracia exige la correspondencia entre los que toman las decisiones políticas y los que están sometidos a ellas. Así entonces, es indudable que todo ejercicio de un poder público representa un ejercicio de la soberanía del Estado.

También es verdad que todo poder público "constituido" por la Constitución es democrático. Para Schmidt-Assmann, todas las Instituciones Públicas deben ser consideradas portadoras de poder estatal, "Todo poder estatal deriva del pueblo. Se ejercita por el pueblo en elecciones y votaciones y a través de especiales órganos de los poderes legislativo, ejecutivo y judicial". Para este autor, cualquier poder estatal, "*staatsgewalt*", cualquier unidad administrativa que tenga una potestad de decisión o de autoconfiguración, *"selbstdarstellung"* requiere una legitimación democrática[582].

Por consiguiente, la independencia de una entidad administrativa, como lo es la autoridad de control en materia de protección de datos, está determinada por las funciones que realiza en pos de alcanzar el fin que le es propio, garantizando la prevalencia de los criterios técnicos y jurídicos como fundamentos de la decisión que adopte.

Así entonces, las funciones que desarrollan estos órganos de la Administración se enmarcan en los significados positivos del término neutralidad de Schmitt, que favorecen la toma de decisiones, decisiones que no serán políticas sino jurídicas, técnicas, arbitrales: en una palabra, neutrales. La neutralidad de los distintos órganos es similar a la neutralidad del Juez que decide sobre la base de una ley reconocida con contenido determinable, la neutralidad de un experto que dictamina atendiendo a criterios que le vienen dados por la ciencia y la neutralidad del árbitro o del tercero que, manteniéndose al margen de los antagonismos de las partes, es capaz de consensuar y de ser cauce de una decisión.

La independencia y neutralidad de las entidades administrativas implica también que sus órganos directivos en cuanto a su nombramiento y destitución están sustraídos o en el peor de

---

de Derecho Administrativo", Vol. I, op. cit. p. 414; Jiménez-Blanco, A. (1989), *"Derecho Público del Mercado de Valores"*, Ceura, Madrid, p. 22; Sala Arquer, J.M. (1985), *"El Estado neutral. Contribución al estudio de las administraciones independientes"*. Así también, para-Greenwood, con independencia de las peculiaridades de cada Administración independiente, *"the desire to distance important areas of public administration from direct political control hasbeen a major factor in the twentieth-century growth of quasi-government."* Greenwood, J. & Wilson, D. (1989), "*Public Administration in Britain Today"*, Unwin Hyman, London, 2º ed., p. 210.

[582] Schmidt-Assmann, E. (1993), "La legitimación de la Administración como concepto jurídico", *Documentación Administrativa*, n° 234, 1993, pp. 172-183.

los casos alejados de la decisión exclusiva del Gobierno. Y especialmente se expresa esa independencia en la inamovilidad durante un periodo determinado de tiempo de la o las instancias decisorias y dirección que tengan[583].

La protección o tutela de los derechos fundamentales en materias vinculadas a las tecnologías de la información, así como al derecho de los consumidores, requiere el establecimiento de organismos independientes, especialmente si los derechos afectados son aquellos vinculados a la esfera íntima de la persona, como son el derecho a la intimidad, a la protección a la vida privada o a la honra. Como se ha señalado, la privacidad es más amplia que la intimidad, esta última se refiere a los ámbitos más reservados de la persona, tales como su domicilio, las comunicaciones donde expresa sus pareceres y sentir. En cambio, la privacidad, al ser más amplia, considera un conjunto de aspectos de la persona que aislados pueden carecer de significación o relevancia, pero que, ordenados sistémicamente, pueden arrojar la identificación de una persona, la que tiene derecho a mantener en reserva dichos aspectos que le individualizan[584].

En este mismo sentido, como se sabe, el artículo 18.4 de la Constitución Española[585] establece que "La Ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de los derechos". Por lo que el derecho a la protección de datos personales nace frente a los peligros que la informática supone para los derechos y libertades de las personas, por cuanto las organizaciones públicas y privadas solicitan cada vez más datos personales, que son tratados de manera automatizada, para incrementar la eficacia de su actividad.

Los medios informáticos tienen la capacidad de archivar una cantidad ilimitada de información, que después puede ser fácil y rápidamente accesible. Así ya lo declaraba el Tribunal Constitucional Federal Alemán, en su sentencia del 15 de diciembre de 1983: "Los procesos de decisión ya no se pueden retrotraer como antiguamente a registros y documentos compilados manualmente; antes bien, hoy día, gracias a la ayuda de la elaboración automática de datos, la información individual sobre circunstancias personales u objetivas de una persona

---

[583] La independencia y neutralidad pretendida no va dirigida a separar a la Administración de los intereses sociales en conflicto, ni tampoco a evitar la parcialidad, es decir el beneficio a una de las partes, en los sectores sociales afectados: es, por, sobre todo, una neutralidad frente a la dirección política del Estado, para poder desempeñar las funciones sin sentirse condicionados por este.

[584] En 1873, el juez Cooley, en su obra *"The Elements of Torts"*, lo definió como *"the Right to be alone"*. Como ya se señaló en este trabajo, la formulación de la *Right of privacy* aparece por vez primera en un artículo publicado en 1890 en la Harvard Law Review por Samuel D. Warren y Louis D. Brandes bajo el tículo: *"The Right of privacy"*. Es por consiguiente un derecho frente a los poderes públicos y frente al resto de los ciudadanos. Este derecho ha fundamentado la declaración de inconstitucionalidad de las leyes que penalizaban el uso de anticonceptivos y el aborto; en efecto en Griswold v. Connecticut 381 US 479, 196, el Juez Douglas estimó que existe una íntima relación entre marido, mujer y médico, en la que no deben entrometerse los poderes públicos. Sobre la *Right of privacy*, véase Wolfe, C. (1986), *"La transformación de la interpretación constitucional"*, Cívitas, Madrid; y García, A. L. (1984), *"La interpretación de la Constitución, Centro de Estudios Constitucionales"*, Madrid.

[585] Y si bien, la CE no se refiere al derecho a la privacidad, sino que sólo se refiere expresamente al derecho al honor, a la intimidad personal y a la propia imagen, a la inviolabilidad del domicilio y al secreto de las comunicaciones a los que confiere un reconocimiento como derechos fundamentales en los tres primeros incisos del art. 18. Evidenciando que estos tres derechos se relacionan estrechamente por cuanto se refieren a ámbitos reservados de la persona del que están excluidas las demás correspondiendo a cada cual el compartirlos o no.

determinada o, en su caso, determinable son técnicamente hablando acumulables sin límite alguno y en cualquier momento se pueden recabar en cuestión de segundos, cualquiera que sea la distancia"[586].

No hace tantos años atrás la privacidad y la esfera personal de cada individuo estaban protegidas por el tiempo y por el espacio, en efecto, el transcurso del tiempo permitía que los hechos ocurridos se olvidaran evitando el desarrollo de una historia lineal e ininterrumpida de la persona; a su vez la distancia impedía que se conocieran los hechos ocurridos en un lugar distinto. Esos límites han desaparecido por las tecnologías de la información, la informática y la inteligencia artificial, lo que permite un conocimiento completo del individuo, al que solo debe de tener acceso él mismo o aquellos a los que él autorice. El acceso a esa información ordenada y sistematizada puede dibujar un determinado perfil de la persona o incluso incidir en su reputación o fama.

Dicha información puede y es utilizada por entidades públicas y privadas para tomar decisiones, incluso esta información y su tratamiento informático es utilizado como técnica de acumulación de datos para controlar o incidir en determinados comportamientos ideológicos y políticos, lo que supondría un grave atentado a los derechos fundamentales, por lo que es imprescindible establecer sistemas de garantías que tutelen y protejan la intimidad, privacidad y datos de los ciudadanos.

De esta manera, la informática y el desarrollo tecnológico tienen una doble dimensión, por una parte son una amenaza para los derechos fundamentales, por cuanto a través de ellos se desarrolla el tratamiento de datos que puede vulnerar la intimidad y privacidad de las personas, y por otro lado contribuyen al ejercicio de funciones públicas tan esenciales para la salvaguarda de los derechos e intereses de la colectividad como son, por ejemplo, las funciones de policía, defensa nacional, o ahora en los tiempos de pandemia, las sanitarias e inspectoras, las que solo pueden desarrollarse con eficacia y eficiencia a través de bases de datos.

A su vez se debe entender que el derecho fundamental a la protección de datos personales representa un derecho autónomo respecto del derecho a la intimidad personal, al proteger también los datos que no pertenecen a la intimidad de la persona, pues tutela a todos aquellos datos que corresponden a cada individuo y que al tratarse automatizadamente podrían dañar otros derechos fundamentales (honor, intimidad, presunción de inocencia…) y bienes jurídicamente protegidos (bienes económicos, culturales…), configurándose como una libertad informática o autodeterminación informativa que confiere al titular de los datos un derecho a controlarlos.

Para garantizar adecuadamente el derecho de protección a los datos personales, como se ha señalado existen diversos mecanismos, uno de ellos es el establecimiento de órganos de control, y concretamente, el de la configuración de agencias o entidades independientes, las que como se ha visto pueden conformarse a través de diferentes modelos y estructuras.

[586] Ver en: http://www.derecho-chile.cl/sentencia-de-15-de-diciembre-de-1983-del-tribunal-constitucional-federal-aleman-ley-del-censo/ consulta realizada el 23 de junio de 2020.

CAPÍTULO V

HACIA LA INSTITUCIONALIZACIÓN DE LA PROTECCIÓN DE DATOS PARA CHILE

La Privacidad y la protección a la Vida Privada en las Constituciones chilenas

Desde los inicios de la historia republicana en Chile y con la conformación de un incipiente ordenamiento jurídico, es posible distinguir una preocupación por proteger la vida privada y por consiguiente la información de carácter personal de los ciudadanos. Así se puede colegir de la revisión de las Constituciones chilenas, que son posibles de agrupar en tres grandes periodos históricos. El primero se podría extender entre 1811 y 1833, período histórico de búsqueda y de ensayo de diferentes modelos constitucionales, predominando una cierta inestabilidad política que derivó en la dictación de varias constituciones, la de 1811, la de 1812, la de 1814, la de1818, la de 1822, la de 1823, la de 1826 y la de 1828.

En segundo lugar, se distingue un período que abarca desde 1833 a la actualidad y que estaría llegando a su fin, marcado por una mayor estabilidad constitucional y con tres constituciones, caracterizadas por su capacidad de duración, flexibilidad y acomodo a las circunstancias históricas (Cartas de 1833, 1925 y 1980).

El tercero y último, es el actual periodo que se puede denominar de transición, en el que Chile después de enfrentar un plebiscito el 25 de octubre del año 2020, decidió por una abrumadora mayoría avanzar hacia la elaboración de una nueva Constitución para el país[587], proceso que debería culminar con un plebiscito ratificatorio del nuevo texto constitucional que se proponga, cuya fecha está fijada para el 4 de septiembre del año 2022.

A continuación, se revisará cómo las constituciones chilenas, de manera incipiente primero, abordaron la protección a la privacidad y vida privada, para culminar en el reconocimiento de la protección de datos de carácter personal como un derecho fundamental.

Reglamento Constitucional de 1812

Es promulgado el 26 de octubre de 1812, bajo el Gobierno de José Miguel Carrera. Se estructura en base a un Preámbulo y 27 artículos, que incluyen diversos conceptos políticos modernos, tales como el de soberanía nacional, régimen representativo, división de poderes públicos y garantías individuales de las personas, entre otros, es considerado el primer texto

[587] El 78,27% de los ciudadanos que votaron en el Plebiscito, aprobaron iniciar el proceso de redacción de una nueva Constitución, mientras que el órgano encargado de hacerlo será la Convención Constitucional, que se impuso a la opción de la Convención Mixta por un 78,99%. Ver en: **¡Error! Referencia de hipervínculo no válida.** consulta realizada el 06 de enero de 2021

constitucional chileno. Fue derogado el 6 de octubre de 1813[588]. En relación con la privacidad su artículo 16 dispone:

> *"Se respetará el derecho que los ciudadanos tienen a la seguridad de sus personas, casas, efectos y papeles; y no se darán órdenes sin causas probables, sostenidas por un juramento judicial, y sin designar con claridad los lugares o cosas que se han de examinar o aprehender".*

Constitución de 1818

Promulgada el 23 de octubre de 1818, durante el gobierno del Director Supremo Bernardo O'Higgins. Dejó de regir el 30 de octubre de 1822, durante la misma administración. Esta Constitución consagra el principio de soberanía popular que otorga a la Nación la facultad de instalar su gobierno y dictar las leyes que lo han de regir. Reconoce asimismo la separación de poderes. El Poder Ejecutivo es ejercido por el Director Supremo con amplias atribuciones. El Poder Legislativo, conformado por un Senado de cinco vocales designados por el Director Supremo tiene como función velar por la observancia de la Constitución y las leyes. El Poder Judicial, por su parte, es entregado a un Supremo Tribunal Judiciario y a una Corte de Apelaciones y juzgados subalternos[589].

En lo relativo a la privacidad, su artículo 5° dispone:

> *"La casa y papeles de cada individuo son sagrados, y, esta ley sólo podrá suspenderse en los casos urgentes en que lo acuerde el Senado".*

Y luego el artículo 11 establece que:

> *"Todo hombre tiene libertad para publicar sus ideas y examinar los objetos que están a su alcance, con tal que no ofenda a los derechos particulares de los individuos de la sociedad[590], a la tranquilidad pública y Constitución del Estado, conservación de la religión cristiana, pureza de su moral y sagrados dogmas; y en su consecuencia, se debe permitir la Libertad de imprenta, conforme al reglamento que para ello formará el Senado o Congreso".*

Constitución de 1822

Se promulga el 30 de octubre de 1822, durante el gobierno de Bernardo O'Higgins. Dejó de regir el 28 de enero de 1823, fecha de su renuncia al cargo de Director Supremo. El texto consta

---

[588] Ver en: https://www.bcn.cl/historiapolitica/constituciones/detalle_constitucion?handle=10221.1/17607 consulta realizada el 25 de septiembre de 2020.

[589] Ver en: https://www.bcn.cl/historiapolitica/constituciones/detalle_constitucion?handle=10221.1/22257 consulta realizada el 25 de septiembre de 2020.

[590] El destacado es nuestro.

de 248 artículos. Dispone que el gobierno de Chile tiene carácter representativo, estando compuesto por tres poderes independientes: Legislativo, Ejecutivo y Judicial. Consagra además las garantías individuales y declara que todos los chilenos son iguales ante la ley, sin distinción de rango o privilegio. Lo novedoso de esta constitución es la adopción de un sistema bicameral compuesto por una Cámara de Diputados, con miembros elegidos, y un Senado, compuesto por distintas personalidades del mundo político, religioso y cultural, como los exdirectores supremos, los miembros de la Corte de Representantes, los ministros de Estado, entre otros[591]. A la privacidad se refiere el artículo 224 al disponer:

> *"Es sagrada la inviolabilidad de las cartas, y la libertad de las conversaciones privadas".*

Constitución de 1828

Promulgada el 8 de agosto de 1828 bajo el gobierno de Francisco Antonio Pinto. Su vigencia se extendió hasta el 25 de mayo de 1833. Es el primer texto que utiliza el título de "Constitución Política de la República de Chile". El texto constitucional está compuesto por 134 artículos distribuidos en 13 Capítulos, establece una tercera alternativa entre el esquema federalista y el autoritarismo centralizador que se discutían en la década de 1820.

La Carta Fundamental consagra como derechos imprescriptibles e inviolables, entre otros, la libertad, la propiedad, el derecho de petición, el de opinión. Asimismo, consagra el principio de la división de los poderes: Ejecutivo, Legislativo y Judicial, encontrándose este último regulado en el Capítulo IX[592].

En lo que respecta a la privacidad el artículo 16 dispone que:

> *"Ninguna casa podrá ser allanada, sino en caso de resistencia a la autoridad legítima, y en virtud de mandato escrito de ella". Y luego el artículo 19 señala que "La ley declara inviolable toda correspondencia epistolar; nadie podrá interceptarla ni abrirla, sin hacerse reo de ataque a la seguridad personal".*

Constitución de 1833

Jurada y promulgada el 25 de mayo de 1833, bajo el gobierno de José Joaquín Prieto. Los autores principales fueron los abogados Manuel José Gandarillas, liberal, y Mariano Egaña, conservador. Reformada en varias oportunidades, a partir de 1865, rigió hasta 1925. Esta Constitución es la de mayor duración en la historia política de Chile, rigiendo casi ininterrumpidamente por noventa y un años. El contexto histórico en el cual se dicta esta Carta

---

[591] Ver en: https://www.bcn.cl/historiapolitica/constituciones/detalle_constitucion?handle=10221.1/17422 consulta realizada el 25 de septiembre de 2020.

[592] Ver en: https://www.bcn.cl/historiapolitica/constituciones/detalle_constitucion?handle=10221.1/18432 consulta realizada el 05 de octubre de 2020.

está marcado por el triunfo del bando conservador sobre el liberal, que se definió en la Batalla de Lircay, el 17 de abril de 1830. Esto trajo como consecuencia el establecimiento, por parte de los conservadores, de una hegemonía política que se extendió por treinta años en el país (1831-1861), que se sostuvo en las ideas políticas del ministro Diego Portales.

Los orígenes del texto constitucional se inscriben en la llamada Gran Convención, instancia que se había convocado originalmente para reformar la Constitución de 1828. Instalada el 20 de octubre de 1831, la Gran Convención estuvo compuesta de 36 miembros, 30 de los cuales eran parlamentarios, la mayoría diputados. Dicha Convención encargó la elaboración del proyecto de Constitución a una comisión de 7 miembros, donde sobresalieron los abogados Mariano Egaña y Manuel José Gandarillas. Entre fines de octubre de 1831 y abril de 1832, esta comisión redactó un primer proyecto, el cual fue revisado por la Gran Convención, junto a un voto particular redactado por Mariano Egaña, quien fue a la postre uno de los principales gestores del texto constitucional final.

Finalmente, el 15 de mayo de 1833, el texto aprobado por la Gran Convención siendo promulgado y jurado por el presidente José Joaquín Prieto[593].

A la privacidad se refieren los artículos 146 y 147, los que señalan:

> *Artículo 146 "La casa de toda persona que habite el territorio chileno es un asilo inviolable, i sólo puede ser allanada por un motivo especial determinado por la lei i en virtud de orden de autoridad competente".*

Por su parte el artículo 147 dispone:

> *"La correspondencia epistolar es inviolable. No podrán abrirse, ni interceptarse, ni rejistrarse los papeles o efectos, sino en los casos espresamente señalados por la lei".*

Constitución de 1925

Se promulga el 18 de septiembre de 1925 por el Presidente Arturo Alessandri Palma, y es sometida a plebiscito el 30 de agosto del mismo año. Pone término al sistema parlamentario estableciendo un régimen presidencialista. A partir del golpe de Estado del 11 de septiembre de 1973, queda subordinada al poder cívico militar.

Esta Constitución se dicta en un contexto de crisis del orden oligárquico parlamentario y de ascenso de los sectores medios y populares, que tuvo su manifestación en la presidencia de Arturo Alessandri Palma (1920-1925). El 3 de septiembre de 1924, la intervención de las fuerzas armadas en la institucionalidad política, y el 12 de marzo de 1925, fecha en la que

[593] Ver en: https://www.bcn.cl/historiapolitica/constituciones/detalle_constitucion?handle=10221.1/17685 consulta realizada el 05 de octubre de 2020.

Alessandri retoma la primera magistratura luego de seis meses fuera del poder, son coyunturas históricas claves para comprender el origen del nuevo texto[594].

En lo que respecta a la privacidad, el artículo 10 numeral trigésimo tercero de la Constitución establecía:

> *"La inviolabilidad de la correspondencia epistolar y telegráfica. No podrá abrirse, ni interceptarse, ni registrase los papeles o efectos públicos, si no en los casos expresamente señalados en la ley"*.

Constitución de 1980[595]

Como antecedentes de la Constitución de 1980, que reemplazó formalmente a la Carta Política de 1925, están las denominadas Actas Constitucionales, en este aspecto es importante precisar que la génesis de la Carta Fundamental se da en el contexto histórico posterior al golpe de Estado del 11 de septiembre de 1973, y del régimen cívico-militar que le siguió. La Junta Militar, mediante los Decretos Leyes N° 1, N° 128 y N° 788, se había atribuido la potestad constituyente, cesando, en los hechos, la vigencia de la Constitución de 1925 y el sistema institucional que la acompañaba.

Así entonces, el Acta Constitucional N° 3 del 11 de septiembre de 1976 consagra por primera vez la protección a la vida privada de las personas.

Esta Carta Política fue promulgada el 21 de octubre de 1980 y publicada tres días más tarde, durante el régimen cívico militar del general Augusto Pinochet Ugarte. Intervienen en su elaboración la Comisión de Estudios de la Nueva Constitución Política, creada por Decreto N° 1064, del Ministerio de Justicia, publicado el 12 de noviembre de 1973, presidida por el abogado Enrique Ortúzar; el Consejo de Estado, creado por Decreto Ley N° 1319, publicado el 9 de enero de 1976; y la propia Junta de Gobierno, integrada por los cuatro altos jefes de las

---

[594] Ver en: https://www.bcn.cl/historiapolitica/constituciones/detalle_constitucion?handle=10221.1/17659 consulta realizada el 05 de octubre de 2020.

[595] Es importante precisar que la Ley N° 21.200, publicada el 24 de diciembre de 2019, que Modifica el Capítulo XV de la Constitución Política de la República, materializó el "Acuerdo por la Paz y la Nueva Constitución", al que llegaron distintos partidos políticos la madrugada del 15 de noviembre de 2019, en el contexto de las movilizaciones sociales iniciadas el 18 de octubre del mismo año. Esta Reforma Constitucional, sienta las bases para permitir la elaboración de una nueva Carta Magna. Establece la realización de Plebiscito Nacional originalmente para el 26 de abril de 2020, en que se consultará a la ciudadanía si "Aprueba" o "Rechaza" elaborar una nueva Constitución y el tipo de órgano encargado de redactarla: "Convención Mixta Constitucional", integrada por parlamentarios y miembros elegidos por votación popular o "Convención Constitucional", integrada en su totalidad por sufragio. Asimismo, regula la forma en que se integra cada uno de estos órganos, sus limitaciones y prohibiciones, el número de convencionalistas. Establece un plazo de 9 meses, que podrá ser prorrogado por 3 meses más, para la elaboración del texto constitucional, el que será enviado al Presidente de la República para que convoque a un Plebiscito Nacional Constitucional para que la ciudadanía lo apruebe o rechace. El Decreto N° 2445 Exento, del Ministerio del Interior, publicado el 27 de diciembre de 2019, convoca al Plebiscito Nacional establecido en la Reforma Constitucional. Finalmente, la cita plebiscitaria se llevó a cabo producto de la pandemia derivada del COVID19, el 25 de octubre de 2020.

Fuerzas Armadas y el Director General de Carabineros. Mediante el Decreto Ley N° 3465, publicado el 12 de agosto de 1980. Para aprobar su texto se convocó a un plebiscito para el día 11 de septiembre de 1980, destinado a que la ciudadanía se pronunciara sobre la nueva Constitución, y entró en vigor el 11 de marzo de 1981, rigiendo hasta la actualidad[596].

En lo que respecta a la vida privada el artículo 19 en su numeral cuarto, hasta el año 2018 establecía:

> *"El respeto y protección a la vida privada y a la honra de su persona y su familia". Luego le numeral 5° del mismo artículo 19 vigente hasta hoy dispone: "La inviolabilidad del hogar y de toda forma de comunicación privada. El hogar solo puede allanarse y las comunicaciones y documentos privados interceptarse, abrirse o registrarse en los casos y formas determinados por la ley".*

Como ya se señaló en el capítulo primero de este trabajo de investigación, el 16 de junio de 2018 se publicó en el Diario Oficial la ley 21.096, que consagra la protección de datos personales como garantía constitucional, en el numeral 4° del artículo 19 de la Constitución chilena, que en la actualidad es el siguiente:

> *"El respeto y protección a la vida privada y a la honra de la persona y su familia y asimismo la protección de sus datos personales. El tratamiento y protección de estos datos se efectuará en la forma y condiciones que determine la ley".*

Consagrando por consiguiente de manera explícita la protección de datos como un derecho fundamental garantizado por la Constitución, separándolo conceptual y normativamente del derecho a la protección a la vida privada. Esa reforma tuvo además por objetivo, según se desprende de la discusión parlamentaria para su aprobación, incidir en el legislador para avanzar en la regulación y reforma del tratamiento y protección de datos personales regulada hasta ahora en la Ley N° 19.628.

Como se puede apreciar, desde los albores de la república, Chile, con más o menos intensidad, abordó la protección de la esfera privada de las personas[597]. En sus orígenes, el "derecho a la vida privada" era concebido como una extensión de la protección del espacio privado, ya sea el hogar, la correspondencia o las relaciones familiares, oponiéndose al concepto de espacio público, en el cual todo individuo podía legítimamente ser objeto de escrutinio. La consideración solía hacerse teniendo únicamente como referencia el espacio en que el sujeto desarrollaba su actividad. Reflejo de lo anterior es la constitución de 1925 en la que se protegía

---

[596] Ver en:https://www.bcn.cl/historiapolitica/constituciones/detalle_constitucion?handle=10221.1/60446consulta realizada el 05 de octubre de 2020.

[597] Incluso en la actualidad, la Convención Constitucional ha formulado una propuesta para que por primera vez se regule el derecho a la privacidad en un texto constitucional chileno. Señala la propuesta: "La protección, promoción y respeto del derecho a la privacidad de las personas, sus familias y comunidades. Ninguna persona ni autoridad podrá afectar, restringir o impedir el ejercicio del derecho a la privacidad salvo en los casos y formas que determine la ley. Los recintos privados son inviolables. La entrada, registro o allanamiento sólo se podrán realizar con orden judicial previa dictada en los casos específicos y en la forma que determine la ley, salvo las hipótesis de flagrancia. Toda forma de documentación y comunicación privada es inviolable, incluyendo sus metadatos. La interceptación, captura, apertura, registro o revisión sólo se podrá realizar con orden judicial previa dictada en la forma y para los casos específicos que determine la ley".

únicamente ámbitos espaciales de la vida privada; la inviolabilidad del hogar y la correspondencia. Esta concepción limitada del concepto de vida privada fue desechada por la constitución de 1980, que consideró "la vida privada" como un objeto especial de protección, distinto a la tradicional institución de inviolabilidad. La concepción más amplia establecida por la constitución de 1980 fue recogida por la jurisprudencia del Tribunal Constitucional chileno, ya que en sus primeras sentencias reconoce el estrecho vínculo que existe entre el derecho a la vida privada y la dignidad de la persona humana, fundamento del sistema de protección de los derechos fundamentales.

Para el Tribunal Constitucional chileno el derecho a la vida privada es un derecho personalísimo, expresión de la dignidad y la libertad humana y que como todo derecho fundamental no es absoluto, quedando sujeto a las limitaciones que se realicen mediante leyes que cumplan con finalidades constitucionales y que hayan sido dictadas conforme a las reglas que ella misma determina[598]. Ahora bien, estas restricciones legales no pueden imponer limitaciones que afecten la esencia del derecho a la vida privada ni imponer limitaciones para su ejercicio, tal como se desprende del numeral 26 del artículo 19 de la Carta Fundamental chilena[599].

En lo que respecta al derecho a la protección de datos personales y su separación del derecho a la vida privada, como lo ha señalado la doctrina, la Comisión de Estudios para la Nueva Constitución no advirtió los riesgos provenientes del desarrollo tecnológico y el tratamiento masivo y automatizado de datos personales, ni tampoco hizo un esfuerzo de deslindar la noción de privacidad (en términos de *privacy*)[600], tal como se entiende en el mundo anglosajón, el cual incluye una noción de privacidad informativa (*information privacy*)[601].

En las siguientes líneas se abordará con mayor detalle la evolución de la protección de datos en Chile, desde su reconocimiento legal a través de la Ley N° 19.628 hasta su reconocimiento constitucional.

[598] "El derecho a la protección de la vida privada no es absoluto y permite limitaciones en vista de la necesidad de proteger un bien jurídico mayor. El legislador este habilitado para regular su ejercicio, sujetándose siempre a la Constitución, la cual le impide afectar el derecho en su esencia, imponerle requisitos o tributos que impidan su libre ejercicio y privarlo de la tutela jurídica que le es debida. La finalidad de la limitación siempre debe ser fundada y razonable". Ver considerando 24° STC 1732.

[599] "La Constitución segura a todas las personas: La seguridad de que los preceptos legales que por mandato de la Constitución regulen o complementen las garantías que ésta establece o que las limiten en los casos en que ella lo autoriza, no podrán afectar los derechos en su esencia, ni imponer condiciones, tributos o requisitos que impidan su libre ejercicio".

[600] Anguita, P. (2007), "*La Protección de Datos Personales y el Derecho a la Vida Privada"*, Editorial Jurídica de Chile, Santiago, p. 136.

[601] Solove, D. J. & Schwartz, P. M. (2018)," *Information Privacy Law"*, New York, Wolters Kluwer, 6° ed, pp. 2-3.

Historia de la Ley sobre protección a la vida privada N° 19.628[602]

Esta ley surge por una moción parlamentaria del año 1993, presentada por el entonces senador Eugenio Cantuarias Larrondo, del 05 de enero, según se registra en la Cuenta de la Sesión 20, de la Legislatura 325, su tramitación excedió los seis años, durante los cuales se discutieron a lo menos tres proyectos distintos, cambiando radicalmente su orientación inicial, desembocando en la regulación del tratamiento de datos personales.

En el texto original del proyecto se establecía que el propósito de este era: "… llenar un vacío manifiesto en nuestro ordenamiento jurídico y cuyo propósito es dar una adecuada protección al derecho a la privacidad de las personas, en el ámbito del Derecho Civil, ante eventuales intromisiones ilegítimas. A diferencia de lo que sucede en otras naciones del mundo, nuestro país carece de una tradición legislativa en esta importantísima materia y en la actualidad no contamos con ningún texto legal expreso que establezca los principios fundamentales por los que se debe regir la labor de nuestros tribunales de justicia a la hora de enfrentar los diversos casos concretos que diariamente se producen en la vida cotidiana y que eventualmente pudieren llegar a plantearse ante dichas instancias jurisdiccionales". Y luego agrega: "…la finalidad de este proyecto es aportar algunos instrumentos específicos que permitan a las personas una efectiva protección de sus vidas privadas ante eventuales atropellos o amenazas de que pudieran ser objeto en el ejercicio de este derecho".

Un aspecto interesante de la moción original es que ya en esos años alertaba sobre la dispersión normativa que existía en Chile para regular y tutelar la vida privada y la intimidad de las personas, y por consiguiente la conveniencia de generar un cuerpo normativo único que regulara de manera integral y sistémica esta materia. Señala el preámbulo de la moción:

"(…) Asimismo, numerosas disposiciones dispersas en nuestro derecho penal, comercial, tributario, civil y procesal incursionan en algunos aspectos puntuales del derecho a la vida privada proyectando algunas consecuencias lógicas que su debida protección y reconocimiento ameritan (…) La clásica dispersión de normas legales existentes a este respecto en nuestro país aconseja la conveniencia de redactar un texto refundido, coordinado y sistematizado sobre la privacidad; una suerte de Código o Estatuto Jurídico de la Privacidad; un cuerpo legal que esté a la altura de esta importantísima institución jurídica. Con todo, esta ardua tarea no se compadece con el vacío legislativo existente en nuestro país, en materia de protección civil de la intimidad, el que es necesario salvar a la mayor brevedad posible, sin perjuicio de dejar planteada la inquietud precedente que inevitablemente se traducirá en una labor de más largo aliento".

Las fuentes normativas que se tuvieron a la vista para la elaboración de este proyecto de ley, fueron entre otras: La ley orgánica Nº1, del 5 de mayo de 1982, de protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen de España; la ley Nº78-17, de 6 de enero de 1978, sobre informática, ficheros y libertades de Francia; la ley de 12 de julio de 1984, sobre protección de datos de Gran Bretaña; la ley Nº48, de 9 de junio de 1978, sobre

[602] Ver en: HLD_6814_37a6259cc0c1dae299a7866489dff0bd.pdf (bcn.cl) consulta realizada el 06 de enero 2021.

registros de datos personales de Noruega; el artículo 1071 bis del Código Civil argentino; y el artículo 9 del Código Civil francés.

Proyecto de ley sobre Protección a la Vida Privada

En su redacción original el proyecto de ley se estructuraba en cinco Títulos y 26 artículos, siendo finalmente el Título II el que adquirió, durante la tramitación legislativa, la mayor importancia ya que abordó la protección de datos personales, que es el contenido principal de la actual ley todavía vigente.

El Título I se refería a algunas disposiciones generales aplicables a la vida privada, partiendo por el precepto contenido en el artículo 19 Nº4 de la Constitución, anunciando la inviolabilidad de la vida privada y advirtiendo que toda intromisión en la misma es, en principio, ilegítima. Se enuncian los principales aspectos a los que ella se extiende, tales como el derecho a la propia imagen; a la intimidad personal y familiar, al anonimato y reserva, a una vida tranquila, sin acosos, hostigamientos ni perturbaciones, y a la inviolabilidad del hogar y de toda forma de comunicaciones privadas. En concordancia con ello, se postula la inadmisibilidad en juicio de los medios de prueba obtenidos mediante intromisiones ilegítimas en la vida privada de una persona, salvo los casos expresamente exceptuados en las leyes. Asimismo, se destina una norma a las informaciones personales obtenidas con ocasión de los sondeos de opinión pública y estudios de mercado, limitándose el uso de dichas informaciones a los fines para los cuales se obtuvieron. Adicionalmente, junto con reconocerse el carácter irrenunciable e imprescriptible del derecho a la privacidad, se salvan los supuestos de autorización legal y de consentimiento del titular. Por último, se ampara la memoria de la persona fallecida, señalándose las personas a quienes corresponde en tales casos el ejercicio de las acciones de protección civil consagradas en la ley, sin perjuicio de las acciones personales a que tienen derecho dichas personas, derivadas de los mismos hechos, cuando hubieren afectado sus propias vidas privadas o la de sus familias.

En el Titulo II se abordaban algunos principios básicos que deben regir en la manipulación de datos personales por medio de la informática. La moción ya en ese entonces reconocía que era "apenas una aproximación a lo que el derecho positivo debe expresar en esta materia". Además, toma como referentes la legislación comparada, principalmente europea, vigentes a la época de su presentación, como las disposiciones contenidas en el artículo 18 Nº4, de la Constitución española (CE), y 35 de la Constitución portuguesa.

> *Artículo 18.4 de la CE; "La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos".*
>
> *Artículo 35 de la Constitución de Portugal; "Utilización de la Informática 1. Todo ciudadano tendrá derecho de acceso a todos los registros informáticos que le conciernen, a requerir que sean rectificados y actualizados, y a ser informado de la finalidad a que se destinan las informaciones, de conformidad con lo dispuesto en la ley. 2. La ley definirá el concepto de "dato personal", junto con términos y condiciones*

> *aplicables a su tratamiento automatizado, vínculos, transmisiones y uso, y garantizará su protección, en particular por medio de un órgano independiente. 3. No se podrá utilizar la informática para el tratamiento de datos referentes a convicciones filosóficas o políticas, afiliaciones a partidos o sindicatos, creencias religiosas, vida privada u orígenes étnicos, salvo con el consentimiento expreso del sujeto, con autorización prevista por la ley y garantías de no discriminación, o con el fin de procesar datos estadísticos que no puedan ser individualmente identificados. 4. El acceso de terceros a los datos personales estará prohibido, salvo en casos excepcionales, de conformidad con la ley. 5. Se prohíbe atribuir un número nacional único a los ciudadanos. 6. Se garantiza a todos el libre acceso a la red informática de uso público. La ley determinará tanto las reglas aplicables al flujo de datos a través de las fronteras como las medidas apropiadas para proteger datos personales y otros que justificadamente hayan de ser salvaguardados en interés nacional. 7. Los datos personales contenidos en archivos manuales disfrutarán de la misma protección prevista en los apartados precedentes, de conformidad con lo dispuesto en la ley"*.

Ya en esos primeros años de la década de los noventa, la iniciativa legislativa sugería la necesidad de legislar a la mayor brevedad posible sobre "la protección de los datos personales contenidos en archivos, registros, bases de datos y ficheros", y reconocía que el proyecto "apenas sienta algunas directrices mínimas que requieren de un necesario complemento mediante una ley específica cuya promulgación no debe dilatarse más allá del tiempo que requiera un estudio acabado y minucioso".

El proyecto original, cuando aún la computación, ni menos las tecnologías de la información alcanzaban el desarrollo vigente en nuestros días, daba cuenta de la potencial afectación de los derechos de las personas mediante el tratamiento de sus datos, cuando señalaba: "Todos los detalles de nuestra vida privada se encuentran en la actualidad archivados en más de algún computador, engrosando voluminosos bancos de datos. Nombre, edad, estado civil, direcciones particular y profesional, integrantes del grupo familiar, sus identidades y colegios donde estudian; enfermedades que han tenido los componentes de la familia, actividades deportivas, culturales y recreativas habituales; ingresos económicos del grupo familiar, cuentas de crédito, corrientes, de ahorro; seguros de vida y de accidentes contratados, patrimonio de bienes raíces y bienes muebles; etcétera. Dichos antecedentes son manejados en la actualidad por bancos, compañías de seguros, administradoras de fondo de pensiones, instituciones de salud previsional, empleadores y casas comerciales, en términos tales que prácticamente los detalles más importantes de nuestras respectivas personas y familias están expuestos hoy a su manipulación por parte de terceros, situación que debe ser regulada por la ley".

Como se puede apreciar, las prevenciones que, en esos años, 1993, hacía la iniciativa legislativa se encuentran más vigentes que nunca, transformándose en una legislación pionera en Latinoamérica, lo que requiere poner en contexto el incipiente desarrollo que en esos años tenía Internet, donde aún ni siquiera era posible imaginar las potencialidades y derivaciones que las TIC y el posterior surgimiento de las Redes Sociales podrían generar. En efecto, desde esos años hasta la fecha, Internet no solo ha transformado de manera sideral la forma de trabajar, de estudiar, de hacer negocios, transferir dinero, hacer trámites de distinto tipo, sino también ha cambiado la forma de relacionarnos y comunicarnos. Utilizando Internet como plataforma, surge la *World Wide Web* (WWW) o red informática mundial que es un sistema de distribución de documentos de hipertexto o hipermedia interconectados y accesibles a través

de Internet. Con un navegador web, un usuario visualiza sitios web compuestos de páginas web que pueden contener textos, imágenes, videos u otros contenidos multimedia, y navega a través de esas páginas usando hiperenlaces. La Web se desarrolló entre marzo del año 1989 y diciembre del año 1990, por el inglés Tim Berners-Lee con la ayuda del belga Robert Cailliau, publicando su trabajo en 1992[603].

Sobre la informática, la moción declara que debe estar al servicio de las personas y que su desarrollo deberá realizarse siempre respetando el derecho a la vida privada de las mismas, ya que, sin perjuicio de las excepciones legales, el proyecto prescribe que nadie podrá utilizar la informática para el procedimiento de datos de índole personal sin el consentimiento de su titular. Por lo que toda persona tiene derecho de acceder a las informaciones que le conciernen y que se encuentren contenidas en registros, bases de datos o archivos, pudiendo exigir se les dé conocimiento de la fuente y del uso a que se destinan dichas informaciones y de rectificar y actualizar las mismas.

Asimismo, la moción señala que "la informática no puede ser utilizada para procesar datos relativos a las convicciones políticas, a las creencias religiosas o a la vida privada, salvo en lo que se refiere al tratamiento con fines estadísticos, de informaciones no identificables. En todo caso, se establece que el usuario deberá tomar las precauciones necesarias para preservar la seguridad de las informaciones contenidas en sus memorias informatizadas e impedir su deformación, daño o transmisión a terceros no autorizados". La moción también establece en el Título II original, que, "toda persona que sufriere un perjuicio por el uso de datos inexactos, incompletos, equívocos, atrasados o caducos, relativos a su persona y que acredite haber ejercitado previamente las acciones que le concede la ley, tiene el derecho a ser indemnizada por el usuario que haya proporcionado tales datos. Junto a un esquema de presunciones simplemente legales, se señalan las normas de procedimiento a que deberán sujetarse estas acciones de indemnización de perjuicios".

El Título III de la moción original sugiere algunos casos en los cuales se estima habría intromisiones ilegítimas en la vida privada de una persona, señalando también algunos casos en que la intromisión no se reputa una conducta antijurídica. En este título el proyecto reconoce la inviolabilidad de la privacidad en todos sus aspectos y reconoce la vigencia de este principio respecto de las personas que ejercen cargos o profesiones de pública notoriedad, respecto de los hechos concernientes a su vida privada. En cuanto a las invasiones a la privacidad cometidas por medios de comunicación, priman las disposiciones de este proyecto respecto de las disposiciones contenidas en la ley de abusos de publicidad de la época. Por último, la moción aclara que hay violación de la intimidad incluso en aquellos casos en que los hechos revelados por el infractor hayan sido dados a conocer ilegítimamente y con anterioridad por otra persona y señala los principios con arreglo a los cuales el titular puede disponer de algún aspecto de su vida privada.

El Título IV de la moción regula la acción de protección, que tiene por finalidad poner término a cualquier injerencia arbitraria o ilegal en la vida privada de una persona, en los mismos términos a lo que se refiere el artículo 20 de la Constitución chilena, cuyo conocimiento y

[603] Oñate Vera, E. (2019), "Internet y la importancia de un órgano de control para la protección de datos personales", en *Revista Rumbos TS*, año XIV, N.º 20, diciembre. ISSN en línea 0719-7721, pp. 189-206.

resolución corresponde a la Corte de Apelaciones respectiva, conforme a las normas de procedimiento establecidas en el Auto Acordado de la Corte Suprema, sobre tramitación del recurso de protección.

La moción original, finalmente, en su Título V se refiere al tribunal competente para conocer de la acción indemnizatoria de perjuicios, que será el del domicilio del demandado[604], es decir, sigue la regla general del ordenamiento jurídico en la materia, contenida en el Código de Procedimiento Civil. Así también, la acción indemnizatoria y las restantes acciones de protección contempladas en el proyecto, se sujetan al procedimiento sumario.

Cada vez que en el proceso conste la intromisión, cuyo carácter ilegítimo se presume legalmente en los casos en que se acrediten el hecho de la injerencia, se debe dar lugar a la acción de resarcimiento de perjuicios, los que también están protegidos por una presunción simplemente legal. Con ambas presunciones el *onus probandi* se invierte, correspondiendo al agresor probar el carácter legítimo de la intromisión o la inexistencia de perjuicios, en su caso.

Etapas de la Tramitación Legislativa

1. A continuación de la presentación de la moción, el mismo día 05 de enero de 1993 se envía oficio a la Corte Suprema de Justicia, que en su parte medular señala: "En atención a que determinadas disposiciones del mencionado proyecto dicen relación con la organización y atribuciones de los tribunales de justicia, el Senado acordó ponerlo en conocimiento de la Excelentísima Corte Suprema, recabando su parecer, en cumplimiento a lo preceptuado por la Constitución Política de la República"[605].

2. Transcurrieron más de dos años desde la presentación del proyecto de ley (05 de enero de 1993) para que la Comisión de Constitución Legislación, Justicia y Reglamento del Senado evacuará su primer informe en 1° trámite constitucional, con fecha 17 de mayo de 1995, como consta en la Cuenta de sesión 63, legislatura 330.

3. Luego, con fecha 07 de junio de 1995, se formulan una serie de Indicaciones (modificaciones), contenidas en el Boletín N- 896-07 (I), indicaciones formuladas

[604] Es importante consignar que durante la discusión del proyecto se promovió en la Comisión de Constitución, Legislación y Justicia del Senado la indicación que proponía que el Juez competente fuese el de domicilio del demandante, alternado con ello la regla general en materia de competencia de los tribunales en Chile. Se extrae del Boletín N°896-07 del 05 de septiembre del 1995, en relación con el artículo 13 del proyecto de ley, lo siguiente: "La Comisión tuvo presente que la indicación, al igual que la norma aprobada en el primer informe que declara competente al tribunal del domicilio del demandante, constituye una modificación a la regla general en materia de competencia relativa, que establece que el tribunal competente para conocer una demanda es el del domicilio del demandado. El motivo que justificarla esta alteración de las reglas generales de la competencia es el de beneficiar a aquellas personas cuyo domicilio está ubicado en una ciudad distinta de aquella en que lo tiene la persona o empresa que comete la infracción a las normas legales en esta materia, por estimarse que, en la Generalidad de los casos, las empresas tendrán su domicilio en la ciudad de Santiago, y, en consecuencia, las personas domiciliadas en provincia verían dificultada su posibilidad de accionar judicialmente".

[605] Oficio de Cámara de Origen a Corte Suprema N° 3802, Solicita opinión sobre proyecto de ley de fecha 05 de enero de 1993.

durante la discusión general del proyecto de ley sobre protección a la vida de las personas.

4. Posteriormente con fecha 07 de junio de 1995, en el Senado en la Legislatura 331, Sesión 05, se aprueba en general el proyecto de ley, estableciéndose como plazo para presentar indicaciones (modificaciones) el medio día del 21 de junio de ese mismo año.
5. El segundo Informe de la Comisión de Constitución del Senado se evacúa con fecha 05 de septiembre de 1995. Según se registra en la Cuenta de la Sesión 31, Legislatura 331. Informe contenido en el Boletín Nº896-07 de la Comisión de Constitución, Legislación, Justicia y Reglamento.
6. A continuación, en la Sala del Senado, se retoma la discusión en particular del proyecto, quedando pendiente, según se registra en la Legislatura 331, Sesión 37, de fecha 14 de septiembre de 1995.
7. Luego, con fecha 03 de octubre de 1995 el Senado aborda la discusión en particular del proyecto, aprobándolo en la Sala según se registra de la Legislatura 332, Sesión 01.

El proyecto aprobado en el Senado puede resumirse de la siguiente manera:

Consta de un total de 16 artículos, agrupados en cuatro títulos. El título I, denominado "Disposiciones Generales", comprende cuatro artículos. El artículo 1° se limita a señalar que el respeto y protección a la vida privada y a la honra de la persona y de su familia se sujetará a las disposiciones de esta ley, sin perjuicio de lo que establezcan otras leyes especiales. El artículo 2° dispone que la vida privada comprende, entre otros aspectos, el respeto a la propia imagen, a la intimidad personal y familiar y a la inviolabilidad del hogar y de toda forma de comunicaciones. El artículo 3° impide que una decisión judicial pueda fundarse en hechos o antecedentes obtenidos por medio de intromisiones ilegítimas en la vida privada de una persona, sin perjuicio de las excepciones legales. El artículo 4° prohíbe difundir o dar a conocer, aun privadamente, los datos de índole personal proporcionados por una persona con ocasión de estudios de mercado o sondeos de opinión pública, de modo tal que permitan identificarlas.

El título II, denominado "De la protección de datos", comprende los artículos 5° al 9°. El artículo 5° dispone que la informática debe estar al servicio de las personas y su desarrollo debe realizarse respetando el derecho a la vida privada y honra de las personas. El artículo 6° señala que el que procese, legítimamente, datos relativos a la vida privada de las personas, sólo puede revelarlos o utilizarlos para aquellas finalidades que hayan sido autorizadas por la ley o consentidas por los afectados. El artículo 7° reconoce el derecho de toda persona a que se le suministre por el usuario de datos procesados a través de la informática, una copia de los antecedentes que tenga en su poder, con indicación de su fuente de origen, en un plazo de cinco días contado desde la solicitud. El artículo 8° consagra similar derecho respecto de los datos personales. Si estos fueren inexactos, incompletos, equívocos o atrasados, la persona tiene derecho a exigir que se rectifiquen, completen, aclaren o actualicen, debiendo proporcionársele copia del registro modificado. La persona también puede exigir que se supriman tales antecedentes, si estuvieren caducos o hubieren sido obtenidos fuera de los casos autorizados por la ley. Lo mismo puede hacer si habiendo proporcionado sus datos personales voluntariamente, no deseare continuar figurando en el registro respectivo. El artículo 9°

reconoce el derecho de la persona afectada por el uso de datos personales incorrectos, a ser indemnizada por quien los haya proporcionado.

El título III, denominado "De las intromisiones ilegítimas en la vida privada", comprende los artículos 10 al 12. El artículo 10 señala que constituye intromisión ilegítima todo acto u omisión arbitrario o ilegal que perturbe, amenace o prive a una persona del ejercicio legítimo del derecho a su vida privada. El artículo 11 dispone que las intromisiones ilegítimas a través de un medio de difusión se rigen por la Ley de Abusos de Publicidad. El artículo 12 precisa que la difusión de hechos concernientes a la vida privada de una persona, con infracción a lo dispuesto en esta ley, no los priva de su carácter privado ni impide al afectado ejercer las acciones pertinentes, si se siguieren difundiendo.

El título IV, denominado "De las acciones a que den lugar las infracciones a la presente ley", comprende los artículos 13 al 16. El artículo 13 señala que es juez competente para conocer de las infracciones a las normas de esta ley, el del domicilio del demandado. Las acciones pertinentes se sujetan a las reglas del juicio sumario y la prueba se aprecia en conciencia. El artículo 14 dispone que toda infracción da derecho al perjudicado para demandar perjuicios por los daños materiales y morales que le haya causado. La acción misma puede interponerse conjuntamente con la demanda destinada a establecer la infracción. En el caso del daño moral, la indemnización la fijará prudencialmente el tribunal, considerando las circunstancias del caso y la gravedad de los hechos. El artículo 15 se pone en el caso de fallecimiento del afectado, evento en el cual las acciones las pueden ejercer sus sucesores, dentro de un plazo no superior a diez años desde el deceso. El artículo 16 permite que el juez pueda apremiar al usuario de datos procesados a través de la informática, si se niega a entregar copia a la persona afectada, en los casos indicados en los artículos 7° y 8°.

8. Con fecha 04 de octubre de 1995 se remite Oficio N° 9093 de Cámara de Origen (Senado) a Cámara Revisora (Cámara de Diputados) donde se comunica que el texto del proyecto de ley fue aprobado en el Senado, registrándose en la Cuenta en Sesión 03, de la Legislatura 332.
9. En segundo trámite constitucional el proyecto pasa a la Cámara de Diputados (cámara revisora) específicamente a la Comisión de Constitución, Legislación y Justicia, la que evacúa su primer informe con fecha 20 de mayo de 1996, según se registra en la Cuenta en Sesión 03 de la Legislatura 333, Boletín 896-07 (S)-1.

En esta instancia se adopta una decisión trascendental para la futura ley, en el sentido de ajustar el proyecto exclusivamente a la protección de datos personales; en efecto, se desprende del texto de la Comisión textualmente lo siguiente: "Sin perjuicio de lo anterior, se acordó circunscribir el proyecto a la normativa relativa a la protección de los datos de carácter personal, ya que el tema de la vida privada de las personas se ha abordado en gran parte en el proyecto sobre libertades de opinión y de información[606]. Se encomendó a la Secretaría de la

[606] Efectivamente el proyecto sobre las libertades de opinión y de información, contenía algunas disposiciones relacionadas con este tema, tales como: El artículo 21, incisos cuarto y quinto, de dicho proyecto, que dispone: "Toda persona tiene derecho a que se corrijan las inexactitudes, omisiones y falsedades de los datos que sobre ella se encuentren registradas en alguna base de datos computacionales, pública o privada, acreditando tal

Comisión hacer un texto comparado entre el proyecto, la normativa aprobada en el proyecto sobre libertades de opinión y de información y los artículos 161-A y 161-B del Código Penal, incorporados a ese cuerpo legal en virtud de una moción del Senador Otero".

> *"Articulo 161-A. Se castigará con la pena de reclusión menor en cualquiera de sus grados y multa de 50 a 500 Unidades Tributarias Mensuales al que, en recintos particulares o lugares que no sean de libre acceso al público, sin autorización del afectado y por cualquier medio, capte, intercepte, grabe o reproduzca conversaciones o comunicaciones de carácter privado; sustraiga, fotografíe fotocopie o reproduzca documentos o instrumentos de carácter privado; o capte, grabe, filme o fotografíe imágenes o hechos de carácter privado que se produzcan, realicen, ocurran o existan en recintos particulares o lugares que no sean de libre acceso al público. Igual pena se aplicará a quien difunda las conversaciones, comunicaciones, documentos, instrumentos, imágenes y hechos a que se refiere el inciso anterior. En caso de ser una misma la persona que los haya obtenido y divulgado, se aplicarán a ésta las penas de reclusión menor en su grado máximo y multa de 100 a 500 Unidades Tributarias Mensuales. Esta disposición no es aplicable a aquellas personas que, en virtud de ley o de autorización judicial, estén autorizadas para ejecutar las acciones descritas.*
>
> *"Articulo 161-B. Se castigará con la pena de reclusión menor en su grado máximo y multa de 100 a 500 Unidades Tributarias Mensuales, al que pretenda obtener la entrega de dinero o bienes o la realización de cualquier conducta que no sea jurídicamente obligatoria, mediante cualquiera de los actos señalados en el artículo precedente. En el evento que se exija la ejecución de un acto o hecho que sea constitutivo de delito, la pena de reclusión se aplicará aumentada en un grado."*

La señalada ley, es la actualmente vigente ley sobre Libertades de Opinión e Información y Ejercicio del Periodismo N° 19.733, publicada el 04 de junio del 2001 y que en sus artículos 16, 17 y 18, se refiere al derecho de rectificación o aclaración.

> *"Artículo 16.- Toda persona natural o jurídica ofendida o injustamente aludida por algún medio de comunicación social, tiene derecho a que su aclaración o rectificación*

circunstancia a través de medios probatorios suficientes y, hecha la rectificación, a que se le otorgue una certificación en que conste la enmienda. Corregida la información, el administrador o responsable del archivo o base de datos computacional la comunicará a la mayor brevedad a quienes el interesado señale y, en su caso, a aquél que la proporcionó originalmente o sirvió de fuente de la información enmendada. El administrador o responsable de un archivo de datos que no haya aceptado la corrección solicitada por la persona que se sintiera afectada, podrá ser requerido a través del procedimiento establecido en el artículo 23, pudiendo ser obligado a efectuar la rectificación, enmienda o complementación por sentencia judicial, y a indemnizar los perjuicios que hubiere causado.". El art. 25 establece: "Toda persona tiene derecho a exigir que los antecedentes, datos o relación de hechos propios de su intimidad o privacidad, amparados por el artículo 19, N° 4°, de la Constitución Política del Estado, sean excluidos de un archivo de datos cuya finalidad sea transferirlos o difundirlos por cualquier medio, a menos que su inclusión tenga un fundamento legal." Su artículo 35 dispone: "Será sancionado con presidio menor en sus grados mínimo a medio y con multa de cien a doscientas unidades tributarias mensuales el que maliciosamente captare palabras o imágenes de otra persona, no destinadas a la publicidad. El que las difundiere, sin el consentimiento del afectado, produciendo a su respecto daño o descrédito será sancionado con presidio menor en cualquiera de sus grados y multa de doscientas a cuatrocientas unidades tributarias mensuales."

sea gratuitamente difundida, en las condiciones que se establecen en los artículos siguientes, por el medio de comunicación social en que esa información hubiera sido emitida".

"Artículo 17.- El ofendido o injustamente aludido por un servicio de radiodifusión sonora o televisiva de libre recepción o un servicio limitado de televisión tendrá derecho, pagando sólo el valor del material que se emplee en la reproducción o proporcionando el que se usará para ello, a requerir directamente la entrega de una copia fiel de la transmisión a que se refiere el artículo 15, la que deberá ser puesta a su disposición dentro de quinto día. En caso de que el respectivo servicio no hiciere entrega de la copia dentro de plazo o se negare injustificadamente a hacerlo, y juez con competencia en lo criminal la estimara pertinente para acreditar un posible hecho delictivo, a solicitud del interesado y a su costa podrá requerir el envío de la copia, para ponerla a disposición de éste. El director responsable o quien lo reemplace deberá entregar al tribunal la copia fiel de la transmisión dentro de tercero día, contado desde que se le notifique la resolución que ordene enviarla".

"Artículo 18.- La obligación del medio de comunicación social de difundir gratuitamente la aclaración o la rectificación regirá aun cuando la información que la motiva provenga de una inserción. En este caso, el medio podrá cobrar el costo en que haya incurrido por la aclaración o la rectificación a quien haya ordenado la inserción.

En este mismo sentido, del análisis realizado por la Comisión de Constitución de la Cámara de Diputados y que consta en las respectivas actas, es posible extraer que la decisión es abordar la protección de datos personales y descartar la elaboración de un marco jurídico general que proteja la privacidad. Los diputados acuerdan que el proyecto de ley en análisis debe centrarse en la información que se registra y almacena por la vía informática. A este respecto señalan: "Se crean, sin control alguno, bancos de datos con el objeto de centralizar la información de las personas en lo que dice relación con su individualización de uso común o general, como el nombre, el domicilio, el estado civil o el lugar de trabajo, la que también se extiende a cuestiones que se apartan directa o indirectamente de los datos de uso general, como son los relativos a la situación financiera, pasatiempos, creencias religiosas y políticas, bienes que se poseen, incluso la marca y el modelo del automóvil adquirido, todo lo cual amerita contar con una legislación especial sobre esta materia".

10. A continuación, la tramitación del proyecto pasa a la Sala de la Cámara de Diputados, donde se inicia la discusión general con fecha 30 de julio de 1996, quedando pendiente su discusión, según se registra en la Legislatura 333, Sesión 20.
11. Luego, con fecha 04 de septiembre de 1996 se retoma la discusión en general del proyecto de ley, en segundo trámite constitucional, el que es aprobado en general en la sala de la Cámara de Diputados, según la Legislatura 333, Sesión 33. Sin embargo, se proponen algunas modificaciones por lo que el proyecto regresa a la Comisión de Constitución pasando al segundo informe.

12. Con fecha 03 de septiembre de 1997, se presenta el Segundo Informe de la Comisión de Constitución de la Cámara de Diputados según se registra en la Cuenta de la Sesión 39, Legislatura 335, Boletín 896-07 (S)-2.
13. A continuación, con fecha 05 de noviembre de 1997 se pasa a la Sala de la Cámara de Diputados, para la discusión en particular, la que queda pendiente según se consigna en la Legislatura 336, Sesión 13.
14. En la misma situación que el punto anterior el proyecto en la sesión 19, de fecha 16 de diciembre de 1997 pasa a la Sala de la Cámara de Diputados, quedando pendiente su discusión en particular, adoptando el acuerdo de que el mismo vuelva a la Comisión de Constitución, Legislación y Justicia para que esta evacúe en un plazo determinado un nuevo informe.
15. El 14 de enero de 1998 la Comisión de Constitución, Legislación y Justicia evacúa el segundo Informe complementario del proyecto de ley contenido en el Boletín N° 896-07 (S)-3 según se registra en la Cuenta de la sesión 27, Legislatura 336.
16. Posteriormente el 20 de enero de 1998 el proyecto vuelve a la Sala de la Cámara de Diputados, para su discusión en particular, éste se aprueba con modificaciones, el que es devuelto al Senado por medio del Oficio N°1808 de la misma fecha, debiendo ser analizado nuevamente por la Comisión de Constitución, Legislación, Justicia y Reglamento del Senado, en Tercer trámite constitucional[607].
17. Con fecha 04 de agosto de 1998 la Comisión de Constitución, Legislación, Justicia y Reglamento del Senado, en Tercer trámite constitucional evacúa su informe, contenido en el Boletín N°896-07, y propone rechazar las modificaciones introducidas por la Cámara de Diputados al proyecto de ley en informe, con excepción de la relacionada con su encabezamiento y en la denominación del título I, que se propone aprobar, esto es; al primero de los títulos del proyecto de ley, aprobado como título I por el Senado, la Cámara de Diputados propone contemplarlo como título preliminar, con la misma denominación de "Disposiciones generales".
18. En la Legislatura 338, sesión 20, de fecha 12 de agosto de 1998, en la Sala del Senado se rechazan las modificaciones formuladas por la Cámara de Diputados, por lo que el proyecto debe pasar a Comisión Mixta, es decir una instancia integrada tanto por senadores como por diputados.
19. Mediante el Oficio N° 12.826, del 17 de agosto del año 1998, de la Cámara de Origen (Senado) a Cámara Revisora (Cámara de Diputados) se comunica el rechazo de las modificaciones
20. El 02 de junio de 1999 la Comisión Mixta (Senado y Cámara de Diputados) evacúa su informe contenido en el Boletín Nº896-07 (S).
21. Con fecha 08 de junio de 1999 se realiza la sesión en la Sala del Senado, donde se aprueba el Informe de la Comisión Mixta.
22. El 09 de junio de 1999 se envía el Oficio N° 14.374 de Cámara de Origen (Senado) a Cámara Revisora (Cámara de Diputados) dando cuenta de la aprobación del Informe de Comisión Mixta.

[607] Entre otros aspectos que la Cámara de Diputados modifico del proyecto original aprobado previamente en el Senado está la incorporación de un título II nuevo, denominado "Derechos de las personas afectadas", que comprende seis artículos, del 16 al 21, inclusive.

23. A continuación, el 15 de junio de 1999 se aprueba en la Sala de la Cámara de Diputados el Informe de la Comisión Mixta.
24. Posteriormente se remite Oficio N°14.447, de fecha 22 de junio de 1999 desde la Cámara de Origen (Senado) al Ejecutivo, comunicando el texto aprobado por el Congreso Nacional para efectos de ejercer la facultad de veto, comunicando el Ejecutivo que no hará uso de dicha facultad.
25. Con fecha 09 de julio de 1999, el Senado (Cámara de Origen), remite mediante Oficio N°14.535 el proyecto de ley al Tribunal Constitucional para que realice el examen de constitucionalidad. Específicamente lo que se solicita es que el Tribunal Constitucional se pronuncie sobre la constitucionalidad del artículo 16 del proyecto de ley, que dispone: "Artículo 16. Si el responsable del registro o banco de datos no se pronunciare sobre la solicitud del requirente dentro de dos días hábiles, o la denegare por una causa distinta de la seguridad de la Nación o el interés nacional, el titular de los datos tendrá derecho a recurrir al juez de letras en lo civil del domicilio del responsable, que se encuentre de turno según las reglas correspondientes, solicitando amparo a los derechos consagrados en el artículo precedente. El procedimiento se sujetará a las reglas siguientes: a) La reclamación señalará claramente la infracción cometida y los hechos que la configuran, y deberá acompañarse de los medios de prueba que los acrediten, en su caso. b) El tribunal dispondrá que la reclamación sea notificada por cédula, dejada en el domicilio del responsable del banco de datos correspondiente. En igual forma se notificará la sentencia que se dicte. c) El responsable del banco de datos deberá presentar sus descargos dentro del quinto día hábil y adjuntar los medios de prueba que acrediten los hechos en que los funda. De no disponer de ellos, expresará esta circunstancia y el tribunal fijará una audiencia, para dentro del quinto día hábil, a fin de recibir la prueba ofrecida y no acompañada. d) La sentencia definitiva se dictará dentro de tercero día de vencido el plazo a que se refiere la letra anterior, sea que se hayan o no presentados descargos. Si el tribunal decretó una audiencia de prueba, este plazo correrá una vez vencido el plazo fijado para ésta. e) Todas las resoluciones, con excepción de la indicada en la letra f) de este inciso, se dictarán en única instancia y se notificarán por el estado diario. f) La sentencia definitiva será apelable en ambos efectos. El recurso deberá interponerse en el término fatal de cinco días, contado desde la notificación de la parte que lo entabla, deberá contener los fundamentos de hecho y de derecho en que se apoya y las peticiones concretas que se formulan. g) Deducida la apelación, el tribunal elevará de inmediato los autos a la Corte de Apelaciones respectiva. Recibidos los autos, en la Secretaría de la Corte, el Presidente ordenará dar cuenta preferente del recurso, sin esperar la comparecencia de ninguna de las partes. h) El fallo que se pronuncie sobre la apelación no será susceptible de los recursos de casación. En caso de que la causal invocada para denegar la solicitud del requirente fuere la seguridad de la Nación o el interés nacional, la reclamación deberá deducirse ante la Corte Suprema, la que solicitará informe de la autoridad de que se trate por la vía que considere más rápida, fijándole plazo al efecto, transcurrido el cual resolverá en cuenta la controversia. De recibirse prueba, se consignará en un cuaderno separado y reservado, que conservará ese carácter aun después de afinada la causa si por sentencia ejecutoriada se denegare la solicitud del requirente. La sala de la Corte Suprema que conozca la reclamación conforme al inciso anterior, o la sala de la Corte de Apelaciones que conozca la apelación, tratándose del procedimiento establecido en

> los incisos primero y segundo, si lo estima conveniente o se le solicita con fundamento plausible, podrá ordenar traer los autos en relación para oír a los abogados de las partes, caso en el cual la causa se agregará a la tabla respectiva de la misma Sala. En las reclamaciones por las causales señaladas en el inciso precedente, el Presidente del Tribunal dispondrá que la audiencia no sea pública. En caso de acogerse la reclamación, la misma sentencia fijará un plazo prudencial para dar cumplimiento a lo resuelto y podrá aplicar una multa de una a diez unidades tributarlas mensuales. La falta de entrega oportuna de la información o el retardo en efectuar la modificación, en la forma que decrete el tribunal, serán castigados con multa de dos a cincuenta unidades tributarias mensuales y, si el responsable del banco de datos requerido fuere un organismo público, el tribunal podrá sancionar al jefe del Servicio con la suspensión de su cargo, por un lapso de cinco a quince días.".

Sobre este punto es importante precisar que a la fecha de este requerimiento al Tribunal Constitucional, estaban vigentes los artículos 82 N° 1°, de la Constitución Política que establecía que es atribución de este Tribunal: "Ejercer el control de la constitucionalidad de las leyes orgánicas constitucionales antes de su promulgación y de las leyes que interpreten algún precepto de la Constitución"[608]; además de los incisos primero y segundo del artículo 74 de la Carta Fundamental[609] vigente, que establecía: "Artículo 74.- Una ley orgánica constitucional determinará la organización y atribuciones de los tribunales que fueren necesarios para la pronta y cumplida administración de justicia en todo el territorio de la República. La misma ley señalará las calidades que respectivamente deban tener los jueces y el número de años que deban haber ejercido la profesión de abogado las personas que fueren nombradas ministros de Corte o jueces letrados.

La ley orgánica constitucional relativa a la organización y atribuciones de los tribunales sólo podrá ser modificada oyendo previamente a la corte Suprema de conformidad a lo establecido en la ley orgánica respectiva".

Correspondiéndole, por consiguiente, al Tribunal Constitucional realizar el control preventivo de constitucionalidad sobre el señalado artículo 16 del proyecto de Ley de Protección a la Vida Privada. Tribunal que mediante el Oficio N°1457 del 06 de agosto de 1999, informa al Presidente del Senado, remitiendo copia autorizada de la sentencia dictada en los autos Rol N° 290 que dispone que los preceptos contenidos en el artículo 16, del proyecto sometido a control, son constitucionales en el entendido que deben interpretarse en conformidad con lo que se ha señalado en el considerando 7° de esta sentencia, esto es que "este Tribunal entiende que la acción que el mencionado artículo 16 confiere al titular de los datos, tiene por objeto solicitar amparo en sus derechos a requerir información, modificación, cancelación o bloqueo de los mismos".

26. Luego de este pronunciamiento de la Judicatura constitucional, mediante Oficio N° 14.769 del 10 de agosto de 1999, dirigido al Presidente de la República, el Senado

[608] Atribución actualmente conferida en el N° del artículo 93 de la Constitución chilena.

[609] Actual artículo 77 de la Constitución.

comunica el texto aprobado por el Congreso Nacional, para la promulgación y posterior publicación de este.

27. Finalmente, con fecha 18 de agosto de 1999 el proyecto de Ley sobre Protección a la Vida Privada es promulgado, publicándose en el Diario Oficial con fecha 28 de agosto de 1999.

Si bien la promulgación de esta ley fue bien recibida en un inicio, las criticas relativas a las deficiencias de su texto no se dejaron esperar, focalizadas principalmente por la forma en que se llevó a cabo su tramitación legislativa, caracterizada por una excesiva incidencia de parte del mundo empresarial, y por una relativa ausencia de voces desde la academia y la sociedad civil. En efecto, de la revisión de las actas de la historia fidedigna de la Ley 19.628 se advierte una importante influencia de grupos, gremios y empresas interesadas en el negocio que significaba ya en esos años, el procesamiento de datos personales, lo que se sumó al desconocimiento de los parlamentarios que la impulsaron, explicado por la incipiente regulación sobre estas materias en Latinoamérica, a pesar de que según se puede desprender del preámbulo del proyecto, se tuvo en consideración la normativa francesa de 1978 y española de 1992, con las cuales existen diferencias sustantivas, a pesar de que los impulsores de la ley expresaron haberse inspirado en dichos cuerpos normativos.

La moción aprobada por el Senado establecía la protección de datos personales frente a su tratamiento por terceros; además, contenía disposiciones relativas a la extensión de la vida privada, sancionaba las intromisiones ilegitimas a esta y otorgaba instrumentos procesales para buscar resarcimiento en el caso de que una persona se viera injustamente afectada. Sin embargo, la Cámara de Diputados reformuló el proyecto original, incidiendo sobre el mismo en algunas de las siguientes materias:

a. Acotó el proyecto a la protección de datos personales, excluyendo las disposiciones relativas a la intromisión de la vida privada, bajo el entendido de que dicha materia sería regulada por el proyecto de ley sobre libertades de opinión e información, que se encontraba en ese momento en tramitación, esto explica por qué la Ley 19.628 se titula "sobre protección de la vida privada", en circunstancias en que solo regula la protección de datos personales, y no otros aspectos relativos a la protección de la intimidad.

b. La idea del proyecto era lograr un estatuto de la privacidad, teniendo como base la Ley Orgánica española N°1, del 5 de mayo de 1982[610], sobre protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen, otorgando así a las personas una efectiva protección civil de estos derechos frente a las agresiones ilegitimas de que fueren objeto[611].

[610] Ver en: Ley Orgánica 1/1982, de 5 de mayo, de protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen. (boe.es) consulta realizada el 13 de enero de 2021.

[611] Conforme al artículo 18.1 de la Constitución, los derechos al honor, a la intimidad personal y familiar y a la propia imagen tienen el rango de fundamentales, y hasta tal punto aparecen realzados en el texto constitucional que el artículo 20.4, dispone que el respeto de tales derechos constituya un límite al ejercicio de las libertades de expresión que el propio precepto reconoce y protege con el mismo carácter de fundamentales. Constitución Española de 1978.

c. Este proyecto comenzaba declarando que la informática debía estar al servicio de las personas y que su desarrollo debía realizarse respetando siempre el derecho a la vida privada, por lo que prohibía la utilización de esta para el tratamiento de datos personales sin consentimiento de sus titulares, salvo las excepciones legales. Se apreciaba ya la idea de considerar a ciertos datos como sensibles, y otorgarles una regulación especial, se establecía el deber de tomar precauciones para la seguridad de las informaciones, reconociéndoles a los titulares de los datos una serie de derechos de acceso, rectificación, cancelación, y oposición, presentes en la actual normativa. Además, se contemplaba la indemnización a los titulares de datos personales por los perjuicios provocados por el uso indebido de los mismos.

d. Resulta también curioso que en la misma moción se señale que solo se establecen directrices mínimas en cuanto a la protección de datos personales que requieren el pronto complemento de una ley específica sobre la materia. El título III de la ley se refiere a una serie de conductas que se estiman intromisiones ilegítimas en la vida privada de las personas, así como aquellas que no serían antijurídicas.

   Los títulos IV y V contienen las acciones civiles, el tribunal competente para conocerlas y las reglas de procedimiento destinadas a poner término a la injerencia arbitraria en la vida privada de las personas y a indemnizar por los perjuicios materiales y morales causados por dicha injerencia.

A pesar de las deficiencias ya señaladas, la ley 19.628 reguló por primera vez la protección de datos personales en el ordenamiento jurídico nacional, siendo una de las primeras legislaciones latinoamericanas en hacerlo. Antes de su publicación, no existían normas que protegieran a los titulares respecto de sus datos personales.

Además, dispuso por vez primera ciertos derechos a favor de los titulares de los datos para modificar, eliminar o bloquear sus datos personales, estableciendo también que las personas para proteger dichos derechos pueden recurrir ante los tribunales civiles regulando un procedimiento para ello.

Sin embargo, los avances tecnológicos han disminuido la eficacia de esta normativa. De hecho, desde que se publicó la Ley N° 19.628, se han presentado más de 70 mociones parlamentarias para perfeccionar el tratamiento de los datos personales.

En definitiva, es posible inferir que este cuerpo legal, contrariamente a lo que su nombre sugiere, no regula orgánicamente todos los aspectos de la vida privada de las personas. Solo regula de manera muy específica el tratamiento de los datos de carácter personal o nominativos

en registros o bancos de datos, y protege la vida privada de las personas solo cuando estas puedan verse afectadas por dicho tratamiento de sus datos.

Esta legislación, mirada desde la perspectiva actual, resulta absolutamente insuficiente, no solo para regular los distintos aspectos de protección que requiere el desarrollo de la vida privada, como fue su idea original, sino que tampoco promueve y tutela la protección de los datos personales, quedando retasada durante su extensa y excesiva tramitación legislativa de más de seis años, la que no dio cuenta del vertiginoso cambio tecnológico y de información, que requiere un masivo almacenamiento de los datos de las personas y el avance que en otros países ha existido desde hace ya varios años en la materia[612].

Reformas a la Ley 19.628

La ley de protección a la vida privada tiene más de veinte años de vigencia, y si bien se le han introducido algunas modificaciones, relacionadas fundamentalmente con el resguardo a información financiera o bancaria, no ha tenido cambios sustanciales ni en su estructura ni en su contenido, resultando imperioso avanzar hacia una nueva legislación que dé cuenta de los cambios tecnológicos, de los avances informáticos y especialmente sea capaza de generar una institucionalidad que promueva y resguarde la protección de los datos de carácter personal.

A continuación, se revisarán las principales reformas introducidas a la Ley N°19.628:

a) Ley N°19.812

Se publica el 13 de junio del año 2002, es una de las primeras modificaciones desde la entrada en vigencia de la ley 19.682, y tiene como principal fin que los datos personales que sean de carácter económicos, comerciales, bancarios y financieros no sean utilizados ni divulgados con el fin de ejercer discriminación a aquellas personas que postulen a un puesto laboral, con ello se modifica el Código del Trabajo en su Art 2°, estableciendo que "ningún empleador podrá condicionar la contratación de trabajadores a la ausencia de obligaciones de carácter económico, financiero, bancario o comercial que, conforme a la ley, puedan ser comunicadas por los responsables de registros o bancos de datos personales; ni exigir para dicho fin declaración ni certificado alguno..."

Lo anterior, ya que la conducta considerada como ilícita, es decir, condicionar la contratación a la ausencia de obligaciones de carácter económico, se concretaba en una etapa precontractual, esta quedaba fuera del ámbito de aplicación del procedimiento de tutela laboral, principal vehículo procesal que les permite a los trabajadores solicitar la intervención de la justicia cuando sus derechos fundamentales se ven afectados.

[612] Ejemplo de ello es la incorporación a la OCDE, en efecto, el 11 de enero de 2010, Chile firmó el Convenio de Adhesión a la OCDE. Entre las buenas prácticas que se nos han recomendado, destaca la "Protección de la privacidad y flujo transfronterizo de datos personales", elemento ausente en nuestra legislación. Esta recomendación busca impulsar el desarrollo de mercados emergentes de nuestra economía, tales como el de *Offshoring* o Servicios Globales.

En síntesis, esta ley modifica el Título III, sobre la utilización de datos personales relativos a obligaciones de carácter económico, financiero, bancario o comercial, prohibiendo la comunicación de información relacionada con deudas contraídas con empresas públicas o privadas que proporcionen servicios de electricidad, agua, teléfono y gas, y asimismo aquellas contraídas con concesionarios de autopistas[613].

También relacionado con datos derivados de obligaciones de tipo económicas, financieras, bancarias o comerciales, en el mismo Título III, se prohíbe la comunicación de dicha información relacionada con obligaciones que se hayan hecho exigibles por más de cinco años o que se encuentren pagadas o extintas por otros modos de extinguir las obligaciones[614].

Por último, respecto al Código del Trabajo, se estableció la prohibición de usar la información comercial y financiera dentro de un proceso de contratación de un trabajador, la cual tampoco podrá ser exigida ni objeto de una declaración, con la única excepción de que el cargo al cual se postula vaya a tener poderes amplios de administración y representación[615].

b) Ley N°20.463[616]

Segunda modificación de la ley 19.682, se publica el 25 de octubre del año 2010, tiene como principal objeto prohibir a los administradores de bases de datos personales de carácter financiero hacer tratamiento de datos relativos a deudas de personas naturales, cuando estas se hubieran producido en el período en que la persona se encontraba sin empleo[617]. Al igual que la modificación anterior, no es sustantiva, ya que lo único que hace es impedir la publicación e intercambio de información financiera relativa a la morosidad producto de deudas contraídas en el período de cesantía, y no aquellas deudas contraídas con anterioridad, cuya morosidad sea producto del desempleo. Por otro lado, si el individuo no se encuentra adscrito a un seguro de cesantía, es de cargo del deudor el certificar su cesantía ante el Boletín Comercial.

c) Ley N°20.521[618]

Esta modificación buscó prohibir la realización de evaluaciones de riesgo comercial que no estuvieren basadas exclusivamente en información objetiva sobre morosidades o protestos de las personas naturales o jurídicas, obligando a los responsables de los datos a eliminar

[613] Artículo 17 Ley N°19.628.

[614] Artículo 18 Ley N°19.629.

[615] Artículo 2° Código del Trabajo.

[616] Publicada el 25 de octubre de 2010. Modifica Ley N° 19.628, suspendiendo por el plazo que indica la información comercial de las personas cesantes. Ver en: https://www.leychile.cl/Navegar?idNorma=1018376

[617] Artículo 17 de la Ley N°19.628.

[618] Publicada el 23 de julio de 2011. Modifica la Ley N°19.628, sobre protección de datos de carácter personal para garantizar que la información entregada a través de predictores de riesgo sea exacta, actualizada y veraz. Ver en: https://www.leychile.cl/Navegar?idNorma=1028013

inmediatamente dicha información, permitiendo asimismo la indemnización de perjuicios respectiva en caso de infracción[619].

Si se llega a infringir esta ley, se faculta a los afectados para demandar compensación por los daños que dicha infracción le hubiera provocado y también podrán solicitar que la información no objetiva sea eliminada inmediatamente de las bases en las que se encuentran contenidos los datos. Es necesario mencionar que dicha modificación es bastante confusa, ya que en ningún momento se define o precisa qué se entenderá por "información objetiva".

d) Ley N°20.575[620]

Se considera una de las modificaciones más importantes que ha tenido la Ley 19.628, fue promulgada el 14 de febrero del año 2012. El principal mérito de esta ley fue consagrar en la legislación chilena el principio de finalidad (ordena que los datos personales solo pueden utilizarse y tratarse para los fines por los cuales fueron recolectados). Cabe mencionar que la creación de esta ley tuvo como objetivo expreso evitar el abuso en el tratamiento de datos personales por parte de distintas entidades, al punto que fue denominada como "Ley DICOM" en alusión a las prácticas de quienes utilizaban los datos consignados en Equifax, heredera de la antigua empresa dedicada al tratamiento de datos e información de carácter comercial.

En concreto, esta norma viene a limitar el uso de la información financiera de las personas, restringiéndose solo para las evaluaciones de riesgo comercial y procesos de crédito, en circunstancias de que dicha información era comúnmente usada para fines distintos de los cuales habían sido objeto durante la recolección de datos.

e) Ley N° 21.214

Esta ley, publicada en el Diario Oficial el 28 de febrero del año 2020, modifica el artículo 17 de la Ley 19.628, en el sentido de prohibir expresamente a los responsables de datos comunicar los siguientes tipos de deudas: 1) aquellas contraídas con instituciones de educación superior del Fondo Solidario de Créditos Universitarios; 2) aquellas adquiridas con bancos o instituciones financieras con cargo al Crédito con Garantía Estatal; 3) aquellas adquiridas en el marco de las líneas de financiamiento con la Corporación de Fomento de la Producción (CORFO) a estudiantes para cursar estudios en educación superior, y 4) en general, cualquier deuda contraída con la finalidad de recibir para sí o para terceros un servicio educacional formal en cualquiera de sus niveles.

Con esta modificación el legislador establece que las deudas educacionales tendrán el mismo tratamiento que las deudas de servicios básicos que ya estaban regulados en la ley de reforma 19.812 previamente analizada.

619 Artículo 9 de la Ley N° 19.628.

620 Publicada el 14 de febrero de 2012. Establece el principio de finalidad en el tratamiento de datos personales. Disponible en: https://www.leychile.cl/Navegar?idNorma=1037366

Además de las señaladas modificaciones, la ley sobre protección a la vida privada ha generado la promoción de otra cantidad de proyectos de ley contenidos en varios Boletines, promovidos tanto por el ejecutivo a través de Mensaje presidencial o vía Moción parlamentaria[621]. A continuación, se expondrá el contenido de algunos de ellos:

a) Boletín N° 6120-07: Propuesto por el ejecutivo al Congreso el año 2008. El proyecto de ley da cuenta que la legislación sobre protección de datos es insuficiente, promoviéndose el reconocimiento explícito de que cualquier tratamiento de información personal debe respetar los derechos del titular, extendiendo también la protección de datos personales a las personas jurídicas. Un importante aspecto de esta iniciativa es que propone establecer como autoridad de control al Consejo para la Transparencia, que pasaría a denominarse "Consejo para la transparencia y protección de datos personales", con la facultad de hacer cumplir las normas establecidas en la

621 Según el artículo 65 de la Constitución chilena: "Las leyes pueden tener origen en la Cámara de Diputados o en el Senado, por mensaje que dirija el Presidente de la República o por moción de cualquiera de sus miembros. Las mociones no pueden ser firmadas por más de diez diputados ni por más de cinco senadores.

Las leyes sobre tributos de cualquiera naturaleza que sean, sobre los presupuestos de la Administración Pública y sobre reclutamiento, sólo pueden tener origen en la Cámara de Diputados. Las leyes sobre amnistía y sobre indultos generales sólo pueden tener origen en el Senado.

Corresponderá al Presidente de la República la iniciativa exclusiva de los proyectos de ley que tengan relación con la alteración de la división política o administrativa del país, o con la administración financiera o presupuestaria del Estado, incluyendo las modificaciones de la Ley de Presupuestos, y con las materias señaladas en los números 10 y 13 del artículo 63.

Corresponderá, asimismo, al Presidente de la República la iniciativa exclusiva para:

Imponer, suprimir, reducir o condonar tributos de cualquier clase o naturaleza, establecer exenciones o modificar las existentes, y determinar su forma, proporcionalidad o progresión;

Crear nuevos servicios públicos o empleos rentados, sean fiscales, semifiscales, autónomos o de las empresas del Estado; suprimirlos y determinar sus funciones o atribuciones;

Contratar empréstitos o celebrar cualquiera otra clase de operaciones que puedan comprometer el crédito o la responsabilidad financiera del Estado, de las entidades semifiscales, autónomas, de los gobiernos regionales o de las municipalidades, y condonar, reducir o modificar obligaciones, intereses u otras cargas financieras de cualquier naturaleza establecidas en favor del Fisco o de los organismos o entidades referidos;

Fijar, modificar, conceder o aumentar remuneraciones, jubilaciones, pensiones, montepíos, rentas y cualquiera otra clase de emolumentos, préstamos o beneficios al personal en servicio o en retiro y a los beneficiarios de montepío, en su caso, de la Administración Pública y demás organismos y entidades anteriormente señalados, con excepción de las remuneraciones de los cargos indicados en el inciso primero del artículo 38 bis, como asimismo fijar las remuneraciones mínimas de los trabajadores del sector privado, aumentar obligatoriamente sus remuneraciones y demás beneficios económicos o alterar las bases que sirvan para determinarlos; todo ello sin perjuicio de lo dispuesto en los números siguientes;

Establecer las modalidades y procedimientos de la negociación colectiva y determinar los casos en que no se podrá negociar, y

Establecer o modificar las normas sobre seguridad social o que incidan en ella, tanto del sector público como el sector privado.

El Congreso Nacional sólo podrá aceptar, disminuir o rechazar los servicios, empleos, emolumentos, préstamos, beneficios, gastos y demás iniciativas sobre la materia que proponga el Presidente de la República.

Ley 19.628 y la aplicación de sanciones administrativas[622]. Este proyecto no ha avanzado desde el 13 de enero 2010, encontrándose en primer trámite constitucional.

b) Boletín 9307-07: Proyecto presentado por un grupo de diputados, el 15 de abril del año 2014, que se encuentra en primer trámite constitucional, sin movimientos en su tramitación desde esa fecha, en la Comisión de Constitución, Legislación y Justicia. El objeto del proyecto es requerir autorización del titular de datos personales, para exhibición de estos en la guía telefónica.

c) Boletín N° 10.133-03: Propuesta iniciada en el año 2015 por una moción parlamentaria en el Senado. Modifica la Ley 19.628 al eliminar de las excepciones la autorización del titular para el tratamiento de datos aquellos datos que sean necesarios para comunicaciones comerciales de respuesta directa o comercialización o venta directa de bienes o servicios. Busca modificar la regulación de la publicidad dirigida o *spam* a través de la reforma de la Ley 19.496 de Protección de los Derechos de los Consumidores, estableciendo un mecanismo de *opt-in*[623] donde solo se puede enviar publicidad directa a aquellas personas que hayan consentido de forma previa y expresa. El proyecto se está tramitando en la Comisión de Economía del Senado y su último hito legislativo tuvo lugar el 01 de septiembre del año 2016.

---

[622] Señala el proyecto en el N° 3 del preámbulo: Establecimiento de una autoridad de control, "el proyecto establece que la autoridad encargada de velar por el cumplimiento de la normativa, tanto la contenida en esta ley, como en otros cuerpos normativos, será el Consejo para la transparencia, creado por la ley N° 20.285. Por ello, dicho Consejo pasa ahora a denominarse "Consejo para la transparencia y protección de datos personales". Este órgano autónomo tendrá entre sus funciones, por de pronto, mantener un Registro Único Nacional de las Bases de Datos. Enseguida, le corresponderá fiscalizar el cumplimiento de las disposiciones sobre tratamiento de datos personales, pudiendo recabar, en cualquier momento, del responsable del respectivo registro o banco de datos, la información que estime pertinente. También tiene la facultad de inspeccionar los registros o bancos de datos personales a efectos de verificar el cumplimiento de las obligaciones que establece la ley; requerir la inscripción de los bancos de datos, que no estén registrados, en el Registro Único Nacional. Un tercer tipo de potestad es la normativa. De ahí que se le faculte para dictar instrucciones de carácter general o particular, respecto de las condiciones de legitimidad de un tratamiento de datos. En cuarto lugar, se le faculta para conocer de las reclamaciones de particulares relacionadas con el ejercicio de sus derechos, señalados en la ley N° 19.628 y en otras normas sobre protección de datos personales, sin perjuicio de las facultades de otras autoridades. En quinto lugar, se le entregan potestades sancionadoras. Así, podrá sancionar a los responsables de los bancos de datos que infrinjan la normativa sobre protección de datos. En sexto lugar, se le faculta para requerir a los responsables y encargados de los tratamientos, previa audiencia de éstos, la adopción de las medidas necesarias para la adecuación del tratamiento de datos a las disposiciones de esta ley y, en su caso, ordenar la cesación de los tratamientos y cancelación del registro, cuando no se ajuste a sus disposiciones. En séptimo lugar, podrá ejercer facultades en beneficio directo de las personas. En este sentido, podrá proporcionar información a las personas acerca de sus derechos en materia de tratamiento de los datos de carácter personal y promover el respeto de los mismos; ejercer el control y adoptar las autorizaciones que procedan para las transferencias internacionales de datos, conforme lo establecido en la ley N° 19628; así como desempeñar las funciones de cooperación internacional en materia de protección de datos personales. Finalmente, se le obliga a entregar una cuenta anual sobre la actividad desarrollada en torno a la protección de datos personales".

[623] El *opt-in* es el acto mediante el cual un usuario interesado en un contenido acepta recibir información vía email.

d) Boletín N° 10512-07: El proyecto ingresado por moción en la Cámara de Diputados a principios del año 2016, propone agregar el número único de identificación conocido como el número de Rol Único Nacional (RUN) y Rol Único Tributario (RUT) al listado de datos que el artículo 2° de la Ley 19.628 menciona como datos personales. De esta forma se busca evitar distintas formas de vulneración a la privacidad y la autodeterminación informativa de los individuos. Esta modificación parece ser más bien simbólica, toda vez que el RUT y el RUN siempre han sido susceptibles de ser considerados datos personales, ya que identifican o hacen identificable a una persona. El proyecto se encuentra tramitándose en la Comisión de Constitución, Legislación, Justicia y Reglamento y su último hito legislativo tuvo lugar el 13 de enero de 2016.

e) Boletín N° 7886-03: El proyecto iniciado por una moción parlamentaria en la Cámara de Diputados a mediados del año 2011, incluye una ampliación en la noción de titulares de los datos, una extensión del concepto de información comercial, la creación de un Sistema de Obligaciones Económicas (SOE). Asimismo, propone el fortalecimiento de los derechos de los titulares de los datos, la regulación de los requisitos de entrada y de salida del mercado de las distribuidoras de información, la regulación de las obligaciones de todos los titulares de datos de obligaciones económicas, entre otras modificaciones. El último hito de tramitación del proyecto tuvo lugar el 17 de junio de 2014.

f) Boletín N° 8589-07: Modifica la Ley 19.628 a fin de obligar a quienes ofrecen cualquier tipo de producto por vía telefónica el comunicar al receptor de la llamada la fuente original que recolectó dichos datos. Del mismo modo, establece la obligación de ofrecer al receptor la posibilidad de solicitar el borrado de las bases de datos. Este proyecto, iniciado mediante moción parlamentaria presentada en el Senado el 12 de septiembre de 2012, no ha avanzado en su tramitación.

g) Boletín N° 7732-07: Prohíbe el envío de comunicaciones comerciales solo a través de mensajes de texto a teléfonos celulares (SMS) que no hayan sido previamente autorizados por el destinatario. El último hito de tramitación de este proyecto tuvo lugar el 16 de junio de 2011, mismo día en que fue ingresado mediante moción ante la Cámara de Diputados.

h) Boletín N° 11037-07: Proyecto de reforma constitucional, iniciado en moción del Senado, que tiene como objeto incorporar un numeral nuevo en el artículo 19 de la Carta Fundamental, para consagrar el derecho al acceso a internet y la especial protección a la vida privada en ambientes digitales. Se propone un nuevo ordinal N°27º[624]. El derecho al acceso a Internet y la especial protección de la vida privada en

[624] Agregase al artículo 19 el siguiente ordinal 27º, "El derecho al acceso a Internet y la especial protección de la vida privada en ambientes digitales. En consecuencia, el Estado promoverá el acceso libre e igualitario a la red

ambientes digitales. En consecuencia, el Estado promoverá el acceso libre e igualitario a la red pública y no podrá suspender ni entorpecer la capacidad de cualquier persona de acceder y utilizar los contenidos ofrecidos a través de esta. El último hito de tramitación de este proyecto tuvo lugar el 08 de mayo de 2018 en la Comisión de Constitución, Legislación, Justicia y Reglamento.

i) Boletín Nº11.092-07, refundido con boletín 11.144-07: En marzo del año 2017 fue presentado vía mensaje presidencial un proyecto de ley que regula la Protección y el Tratamiento de los Datos Personales y crea la Agencia de Protección de Datos Personales (Boletín N°11.144-0), el que se refunde con una iniciativa parlamentaria que había sido previamente presentada en enero de 2017 (Boletín N° 11.092-07), que también apuntaba a fortalecer la protección de datos personales.

   Este es el proyecto más importante de todos los mencionados anteriormente, dado que tiene como objeto la creación de la ley sobre protección de datos personales, buscando derogar la todavía vigente ley 19.628 sobre protección a la vida privada, estableciendo un nuevo esquema normativo que se ajuste a los estándares exigidos por las legislaciones más avanzadas en la materia.

   Actualmente se encuentra en discusión en el Senado en la Comisión de Hacienda en primer trámite constitucional[625]. Tanto a la Comisión de Constitución, Legislación, Justicia y Reglamento del Senado, como a la Comisión de Hacienda han concurrido durante su discusión varios expertos sobre el tema, los cuales expusieron y dieron su opinión realizando nuevas indicaciones al proyecto, reforzando los derechos ARCO (acceso, rectificación, cancelación y oposición); actualizando las definiciones de conceptos que se encontraban difusos, exigiendo un modelo de protección para su tratamiento y regulando las sanciones para los infractores. Durante la discusión se ha reforzado el tema de la seguridad de los datos, especialmente de los llamados datos sensibles, así como los que pertenecen a niños, niñas o adolescentes, también se ha determinado que sucederá al momento de hacer el tratamiento de datos, la forma, el

pública y no podrá suspender ni entorpecer la capacidad de cualquier persona de acceder y utilizar los contenidos ofrecidos a través de esta.

Ninguna persona podrá impedir u obstaculizar la divulgación de información en línea. El Estado no ejercerá control sobre las comunicaciones electrónicas, así como tampoco dará tratamiento ni recolectará masiva o indiscriminadamente datos de las personas, sean éstas nacionales o extranjeras, que puedan ser obtenidos mediante interceptación de la red pública o de otro medio de comunicación.

Sólo un tribunal de justicia, a petición del Ministerio Público, podrá autorizar la interceptación de comunicaciones para la recolección de datos de una persona determinada, siempre que existieren fundadas sospechas, basadas en hechos determinados, de comisión o participación en un hecho punible sancionado con pena de crimen, y en cuanto tal interceptación sea proporcional e imprescindible para la investigación.

La ley determinará la forma legítima en la que podrá darse tratamiento a los datos personales, procurando garantizar la privacidad y el derecho a la autodeterminación informativa de las personas".

[625] Con fecha 05 de enero se reitera la Suma Urgencia.

procedimiento y la persona encargada del mismo, quién cargará con un deber especial de resguardo.

Asimismo el proyecto busca establecer que el tratamiento de los datos de las personas naturales se realice con su consentimiento o que dicho tratamiento lo autorice la ley, reforzando la idea de que los datos personales deben estar bajo la esfera de control de su titular, favoreciendo su protección frente a toda intromisión de terceros y estableciendo las condiciones regulatorias bajo las cuales puede legítimamente efectuarse el tratamiento de tales datos, asegurando estándares de calidad, información, transparencia y seguridad.

De esta forma, el principal desafío regulatorio es equilibrar la protección de los derechos de las personas, especialmente el respeto y protección a la vida privada e intimidad, con la libre circulación de la información, asegurando que las reglas de autorización y uso que se establezcan no entraben ni entorpezcan el tratamiento lícito de los datos por parte de las personas, entidades públicas y empresas.

En un siguiente apartado de este trabajo se analizarán los principales aportes que se han introducido al proyecto de ley actualmente en tramitación en el Senado y que persigue equiparar el tratamiento de datos personales con los estándares internacionales en la materia, tomando principalmente como referencia el Reglamento General de Protección de Datos Personales de la Unión Europea.

j) Boletín Nº12.877-07: Proyecto de ley iniciado en moción parlamentaria de un grupo de diputados, tiene como objetivo establecer el derecho al olvido dentro de algunos registros de datos personales. Busca que los datos sean usados legítimamente, para el fin de autorizar su tratamiento, sin que ello signifique que permanezca en un fichero o base de datos *"ad eternum"*, por el contrario, se busca que cuando se agota la finalidad, o pierde sentido su tratamiento, esta información debe ser olvidada o eliminada como si nunca hubiere existido. Así, es una expresión del derecho de supresión de la información inútil o sin finalidad[626]. El derecho al olvido, en concreto, ha sido debatido

[626] De los considerandos de este proyecto de ley se extrae el propósito de este, cuando señala: "Nuestra legislación contempla normas que enuncian estas premisas y regulan cómo debe hacerse el tratamiento de datos. Esto, sin que exista una conceptualización expresa del marco del derecho al olvido propiamente tal. La excepción a dicha regla la encontramos en el artículo 18 de la ley 19.628, y en el decreto supremo n° 950 del año 1928 del Ministerio de Hacienda. Ambas normas contienen disposiciones sobre la imposibilidad de comunicar datos caducos, es decir, aquellos datos que han permanecido en un fichero por más de 5 años luego de haberse hecho exigible la obligación. No obstante, dichas normas, no se prohíbe la utilización de datos que se encuentran caducados, para la recopilación de información que con posterioridad pueden ser usados al momento de realizar una evaluación crediticia. De esta forma, los principales agentes crediticios, Bancos, Retail, Financieras, pueden obviar estas disposiciones precisamente porque no está consagrada en ninguna norma expresa. Se hace necesario pues una ley que evite el uso, tratamientos y comunicación de datos caducos.

En esto consiste el derecho al olvido comercial que busca consagrarse en este proyecto de ley. Buscamos evitar que los datos comerciales que se encuentra caducados persigan a personas y emprendedores por siempre. Por

fundamentalmente en dos áreas, a saber: los datos personales en las redes sociales y los datos personales en materia comercial. El último hito de tramitación de este proyecto tuvo lugar el 16 marzo de 2020 y se encuentra en el primer trámite constitucional, en segundo informe de la Comisión de Hacienda.

k) Boletín 12.409-03: Proyecto iniciado por Mensaje Presidencial el 24 de enero de 2019, que en lo relativo a la protección de datos, establece un nuevo articulado en la Ley de Protección al Consumidor que le otorga competencia al Servicio Nacional del Consumidor SERNAC, para fiscalizar y velar por el cumplimiento de la Ley de Protección de Datos cuando las actividades de tratamiento de datos se han desarrollado en el contexto de una relación de consumo, además dispone que los organismos fiscalizadores sectoriales que tengan facultades sancionatorias deberán remitir al SERNAC copia de las resoluciones en que impongan sanciones. Con ello, la futura Agencia de Protección de Datos se encontraría en la obligación de remitir al SERNAC copia de aquellas resoluciones en que impongan sanciones a los proveedores. El proyecto se encuentra en Tercer trámite constitucional en la Cámara de Diputados.

El siguiente cuadro resume las diferentes iniciativas contenidas en los respectivos boletines dando cuenta de su año de presentación, el contenido que aborda y la etapa de tramitación en la que se encuentra.

Cuadro N° 6

N° de Boletín	Año	Contenido	**Etapa de tramitación**
Boletín N° 6.120-07	2008	Propone establecer como autoridad de control al Consejo para la Transparencia, que pasaría a denominarse "Consejo para la transparencia y protección de datos personales".	Primer trámite constitucional, sin avances desde el 13 de enero de 2010.
Boletín 9.307-07	2014	El objeto del proyecto es requerir autorización del titular de datos personales, para	Primer trámite constitucional, sin avances desde el 15 de abril de 2014.

ejemplo, si la obligación ya se encuentra extinguida o prescrita, el mercado del crédito no tiene por qué conocer ese dato al momento de evaluar al emprendedor o persona natural".

		exhibición de estos, en la guía telefónica.	
Boletín N° 10.133-03	2015	Busca modificar la regulación de la publicidad dirigida o *spam* a través de la reforma de la Ley 19.496 de Protección de los Derechos de los Consumidores, estableciendo un mecanismo de *opt-in* en donde solo se puede enviar publicidad directa a aquellas personas que hayan consentido de forma previa y expresa	El proyecto se está tramitando en la Comisión de Economía del Senado y su último hito legislativo tuvo lugar el 01 de septiembre del año 2016.
Boletín N° 10.512-07	2016	Propone agregar el número único de identificación conocido como el número de Rol Único Nacional (RUN) y Rol Único Tributario (RUT) al listado de datos que el artículo 2° de la Ley 19.628 menciona como datos personales. De esta forma se busca evitar distintas formas de vulneración a la privacidad y la autodeterminación informativa de los individuos.	El proyecto se está tramitando en la Comisión de Economía del Senado y su último hito legislativo tuvo lugar el 01 de septiembre del año 2016.
Boletín N° 7.886-03	2011	Propone el fortalecimiento de los derechos de los titulares de los datos, la regulación de los requisitos de entrada y de salida del mercado de las distribuidoras de información, la regulación de las obligaciones de todos los titulares de datos de obligaciones económicas, entre otras modificaciones.	El último hito de tramitación del proyecto tuvo lugar el 17 de junio de 2014.
Boletín N° 8.589-07	2012	Obligar a quienes ofrecen cualquier tipo de producto por vía telefónica el comunicar al receptor de la llamada	Este proyecto, iniciado mediante moción parlamentaria presentada en el Senado el 12 de septiembre de

		la fuente original que recolectó dichos datos. Del mismo modo, establece la obligación de ofrecer al receptor la posibilidad de solicitar el borrado de las bases de datos.	2012, no ha avanzado en su tramitación.
Boletín N° 7.732-07	2011	Prohíbe el envío de comunicaciones comerciales solo a través de mensajes de texto a teléfonos celulares (SMS) que no hayan sido previamente autorizados por el destinatario.	El último hito de tramitación de este proyecto tuvo lugar el 16 de junio de 2011, mismo día en que fue ingresado mediante moción ante la Cámara de Diputados.
Boletín N° 11.037-07	2018	Tiene como objeto incorporar un numeral nuevo en el artículo 19 de la Carta Fundamental, para consagrar el derecho al acceso a internet y la especial protección a la vida privada en ambientes digitales.	El último hito de tramitación de este proyecto tuvo lugar el 08 de mayo de 2018 en la Comisión de Constitución, Legislación, Justicia y Reglamento.
Boletín Nº11.092-07[627]	2017	Este es el proyecto más importante de todos los mencionados anteriormente, dado que tiene como objeto la creación de la ley sobre protección de datos personales, buscando derogar la todavía vigente ley 19.628 sobre protección a la vida privada, estableciendo un nuevo esquema normativo que se ajuste a los estándares exigidos por las legislaciones más avanzadas en la materia. Entre otras cuestiones propone la creación de una Autoridad de Control para la regulación de la protección de datos personales.	Actualmente se encuentra en discusión en el Senado en la Comisión de Hacienda en primer trámite constitucional y el pasado 05 de enero el ejecutivo reitera la Suma Urgencia para su tramitación.

[627] Refundido con boletín N° 11.144-07.

Boletín Nº12.877-07	2020	Tiene como objetivo establecer el derecho al olvido dentro de algunos registros de datos personales. Busca que los datos sean usados legítimamente, para el fin de autorizar su tratamiento, sin que ello signifique que permanezca en un fichero o base de datos *"ad eternum"*	El último hito de tramitación de este proyecto tuvo lugar el 16 marzo de 2020 y se encuentra en el primer trámite constitucional, en segundo informe de la Comisión de Hacienda de la Cámara de Diputados.
Boletín 12.409-03	2019	Otorga competencia al Servicio Nacional del Consumidor SERNAC, para fiscalizar y velar por el cumplimiento de la Ley de Protección de Datos cuando las actividades de tratamiento de datos se han desarrollado en el contexto de una relación de consumo, además dispone que los organismos fiscalizadores sectoriales que tengan facultades sancionatorias deberán remitir al SERNAC copia de las resoluciones en que impongan sanciones.	Desde el 03 de diciembre de 2020 se encuentra en Tercer trámite constitucional en la Cámara de Diputados

Fuente: Elaboración propia.

Hacia una nueva Ley de Protección de Datos en Chile (Boletines números 11.144-07 y 11.092-07 refundidos)

Como ya se señaló, el proyecto de ley que se refunde en estos dos boletines constituye uno de los más ambiciosos en cuanto a cambios sustanciales, pues como se anticipa en el título, incluye el establecimiento de una nueva institucionalidad relacionada con la protección de datos, en concordancia con las tendencias regulatorias a nivel global. En efecto, este proyecto incorpora la existencia de una Autoridad de Control en Protección de Datos, tal como muchos países de Europa y América Latina, introduciendo también una serie de obligaciones a los responsables de datos coincidentes con el cambio de paradigma experimentado ya a nivel global, en el Reglamento General de Protección de Datos (RGPD) de la Unión Europea.

Entre las propuestas más relevantes del proyecto de ley, se destacan las siguientes:

1. Desde luego, un aspecto formal, pero importante, es el cambio en la denominación de la ley, sustituyéndose en el nombre de la ley la frase "La Vida Privada" por "Los Datos Personales".

2. El artículo 1° del proyecto de ley referido al objeto y ámbito de aplicación de esta, se refiere también a la protección de datos personales como un derecho fundamental, considerando la reforma al N°4 del artículo 19 de la Carta chilena, que lo incluyó dentro del catálogo de derechos fundamentales. Dispone el señalado artículo primero del proyecto:

> *"Artículo 1° Objeto y ámbito de aplicación. La presente ley tiene por objeto regular la forma y condiciones en la cual se efectúa el tratamiento y protección de los datos personales de las personas naturales, en conformidad al artículo 19 N° 4 de la Constitución Política.*
>
> *Todo tratamiento de datos personales que realice una persona natural o jurídica, incluidos los órganos públicos, debe respetar los derechos y libertades de las personas y quedará sujeto a las disposiciones de esta ley".*

3. El artículo 2° del proyecto de ley que se refiere a las "Definiciones", donde se incorporan y a su vez precisan varios términos relevantes, entre los que destacan:

a. La letra c) agrega el concepto de Comunicación o transmisión de datos personales, señalando que consiste en "dar a conocer por el responsable de datos, de cualquier forma, datos personales a personas distintas del titular a quien conciernen los datos, sin llegar a cederlos o transferirlos".

b. Las letras f) y g) precisan los conceptos de datos personal y datos sensibles respectivamente, conceptualizándolos como: "Dato personal: cualquier información vinculada o referida a una persona natural identificada o identificable. Se considerará identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante uno o más identificadores, tales como el nombre, el número de cédula de identidad, el análisis de elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona, excluyendo aquellos casos en que el esfuerzo de identificación sea desproporcionado".

   "Datos personales sensibles: sólo tendrán esta condición aquellos datos personales que revelen el origen étnico o racial, la afiliación política, sindical o gremial, hábitos personales, las convicciones ideológicas o filosóficas, las creencias religiosas, los datos relativos a la salud, al perfil biológico humano,

los datos biométricos, y la información relativa a la vida sexual, a la orientación sexual y a la identidad de género de una persona natural".

c. La letra i) se refiere a las fuentes de acceso público, por cuanto uno de los aspectos a mejorar de la Ley 19.628 tenía relación con los vacíos que generaba la definición de este concepto, pues prescinde de la licitud en la recogida de los datos como habilitante para su tratamiento. De esta situación da cuenta el proyecto de ley que las define como: "todas aquellas bases de datos o conjuntos de datos personales, cuyo acceso o consulta puede ser efectuada en forma lícita por cualquier persona, siempre que no existan restricciones o impedimentos legales para su acceso o utilización, tales como listas de colegios profesionales, diario oficial, medios de comunicación o los registros públicos que disponga la ley".

d. La letra t) introduce un nuevo derecho derivado de la protección de datos personales, que es el derecho a la portabilidad de estos, en efecto a los derechos de acceso, rectificación, cancelación y oposición ya consagrados en la ley 19.628, se agrega esta garantía, que va en la misma línea de reconocimiento en otros cuerpos normativos comparados, como el Reglamento General de Protección de Datos de la Unión Europea (RGPD). Se define el Derecho a la Portabilidad de los Datos Personales como el "derecho del titular de datos a solicitar y obtener del responsable, una copia de sus datos personales en un formato electrónico estructurado, genérico y común, que permita ser operado por distintos sistemas, y poder comunicarlos o transferirlos a otro responsable de datos".

e. También, replicando la experiencia comparada, principalmente europea y actualizando la legislación al desarrollo de la informática y las nuevas tecnologías, se incorporan al artículo 2° de las definiciones, nuevos términos, con sus respectivas conceptualizaciones, tales como: i) "Cesión de datos personales: transferencia de datos personales por parte del responsable de datos a otro responsable de datos"; ii) "Elaboración de perfiles: toda forma de tratamiento automatizado de datos personales que consista en utilizar esos datos para evaluar, analizar o predecir aspectos relativos al rendimiento profesional, situación económica, de salud, preferencias personales, intereses, fiabilidad, comportamiento, ubicación o movimientos de una persona natural"; iii) "Motor de búsqueda: Mecanismo o sistema informático que permite buscar información en internet, anexarla o indexarla de manera automática, almacenarla temporalmente, y ponerla a disposición de las personas, según un orden de preferencia no aleatorio. En relación con los resultados de búsqueda, el titular de datos personales podrá ejercer el derecho de cancelación contemplado en la presente ley, sin perjuicio de los demás derechos que establece esta ley, cuando correspondan."; iv) "Tercero mandatario o

encargado: la persona natural o jurídica que trate datos personales, por cuenta del responsable de datos".

4. El artículo 3° referido a los principios que deben sustentar el tratamiento de datos personales, incorpora, ahora de manera expresa, el Principio de Finalidad, el Principio de Proporcionalidad y el Principio de Seguridad. Sobre el primero señala el proyecto que: "Los datos personales deben ser recolectados con fines específicos, explícitos y lícitos. El tratamiento de los datos personales debe limitarse al cumplimiento de estos fines. En aplicación de este principio, no se pueden tratar los datos personales con fines distintos a los informados al momento de la recolección, salvo que el tratamiento sea para fines compatibles con los autorizados originalmente; exista una relación contractual o pre contractual entre el titular y el responsable que justifique el tratamiento de los datos con una finalidad distinta siempre que se enmarque dentro de los fines del contrato o, sea coherente con las tratativas o negociaciones previas a la celebración del mismo; el titular otorgue nuevamente su consentimiento; los datos provengan de fuentes de acceso público, y cuando lo disponga la ley".

Respecto del Principio de Proporcionalidad, el proyecto señala que "Los datos personales que se traten deben limitarse a aquellos que resulten necesarios en relación con los fines del tratamiento. Los datos personales deben ser conservados sólo por el período de tiempo que sea necesario para cumplir con los fines del tratamiento, luego de lo cual deben ser cancelados o anonimizados. Un período de tiempo mayor requiere autorización legal o consentimiento del titular".

Sobre el Principio de Seguridad, el proyecto dispone: "En el tratamiento de los datos personales, el responsable debe garantizar estándares adecuados de seguridad, protegiéndolos contra el tratamiento no autorizado o ilícito, y contra su pérdida, filtración, daño accidental o destrucción. Las medidas de seguridad deben ser apropiadas y acordes con el tratamiento que se vaya a efectuar y con la naturaleza de los datos".

5. Un aspecto central que aborda el proyecto de ley es el establecimiento de una autoridad de control en protección de datos, la que no implica la creación de una nueva entidad en la estructura administrativa chilena, sino que se le asigna esta calidad al hasta ahora denominado Consejo para la Transparencia, el que pasaría a denominarse "Consejo para la Transparencia y la Protección de Datos Personales", cuya función será la de velar por el efectivo ejercicio y cumplimiento de los derechos que se le reconocen al titular de los datos, según lo dispuesto en la respectiva legislación y en lo que corresponda, en la ley N° 20.285 sobre Acceso a la Información Pública.

Si bien se considera de la mayor relevancia el establecimiento de una autoridad de control en la materia, por diversas razones y argumentos que se expondrán más adelante, no parece adecuado asignar esta función a una entidad que, desde su creación,

en el año 2008, tiene como función el promover y regular la transparencia y el acceso a la información pública.

6. El proyecto de ley también avanza en un tema fundamental y que resuelve uno de los principales déficits de la actual ley 19.628, que dice relación con el procedimiento para ejercer los derechos derivados de la protección de datos, los denominados derechos ARCO, a los que según el proyecto de ley también habría que agregar el derecho de portabilidad. Este procedimiento, también denominado Habeas Data en la todavía vigente legislación, consiste en una instancia de reclamación judicial ante la imposibilidad o ausencia de respuesta respecto al ejercicio de los derechos ARCO por parte del titular de los datos, tratándose de un proceso engorroso en sede Civil que podía tardar años. El Proyecto modifica su ejercicio, extendiendo el plazo de respuesta establecido para los responsables de los datos, pasando de dos a 15 días hábiles. A lo que se suma una significativa reforma frente a la falta de respuesta del responsable de los datos, por cuanto antes de la vía jurisdiccional para accionar, el proyecto establece una reclamación administrativa directa ante la Autoridad de control, pudiendo el titular exigir el bloqueo temporal del tratamiento mientras dure la tramitación de la reclamación.

El artículo 11 del proyecto de ley, actualmente en tramitación en el Senado sobre esta materia, dispone: Procedimiento ante el responsable de datos. Para ejercer los derechos que le reconoce esta ley, el titular deberá presentar una solicitud o requerimiento escrito ante el responsable, dirigido a la dirección de correo electrónico establecida para este fin, un formulario de contacto o un medio electrónico equivalente. La solicitud deberá contener, a lo menos, las siguientes menciones: a) Individualización del titular y de su representante legal o mandatario, según corresponda y autenticación de su identidad de acuerdo con los procedimientos, formas y modalidades que establezca el Consejo para la Transparencia y la Protección de Datos Personales. b) Indicación de un domicilio o una dirección de correo electrónico o de otro medio equivalente para comunicar la respuesta. c) Identificación de los datos personales o del tratamiento determinado, respecto de los cuales se ejerce el derecho correspondiente. d) En las solicitudes de rectificación, el titular deberá indicar las modificaciones o actualizaciones precisas a realizar y acompañar, en su caso, los antecedentes que las sustenten. Cuando se trate de solicitudes de cancelación, el titular deberá indicar la causal invocada y acompañar los antecedentes que la sustenten, si correspondiere.

Para las solicitudes de oposición, el titular deberá indicar la causal invocada y en el caso de la letra a) del artículo 8°[628], deberá fundamentar brevemente su petición, podrá

[628] Se refiere al Derecho de Oposición. El titular de datos tiene derecho a oponerse ante el responsable a que se realice un tratamiento específico o determinado de los datos personales que le conciernan, en los siguientes casos: a) Si el tratamiento afecta sus derechos y libertades fundamentales.

igualmente acompañar los antecedentes que estime procedentes. En el caso del derecho de acceso, bastará con la individualización del titular.

Recibida la solicitud el responsable deberá acusar recibo de ella y pronunciarse a más tardar dentro de los 15 días hábiles siguientes a la fecha de ingreso.

El responsable deberá responder por escrito al titular a su domicilio o a la dirección de correo electrónico fijada por este. El responsable debe almacenar los respaldos que le permitan demostrar la remisión de la respuesta a la dirección física o electrónica que corresponda, su fecha y el contenido íntegro de ella.

En caso de denegación total o parcial de la solicitud, el responsable deberá fundar su decisión indicando la causa invocada y los antecedentes que la justifican. En esta misma oportunidad el responsable debe señalar al titular que dispone de un plazo de 15 días hábiles para formular una reclamación ante el Consejo para la Transparencia y la Protección de Datos Personales, de acuerdo con el procedimiento establecido en el artículo 41[629].

Transcurrido el plazo de 15 días hábiles sin que haya respuesta del responsable, el titular podrá formular directamente una reclamación ante el Consejo para la Transparencia y la Protección de Datos Personales, en los mismos términos ya señalados.

Cuando se formule una solicitud de rectificación, cancelación u oposición, el titular tendrá derecho a solicitar y obtener del responsable el bloqueo temporal de sus datos o del tratamiento que realice, según corresponda. La solicitud de bloqueo temporal deberá ser fundada y el responsable deberá responder al requerimiento dentro de los dos días hábiles siguientes a su recepción. En tanto no resuelva esta solicitud, el responsable no podrá tratar los datos del titular que forman parte del requerimiento. En caso de rechazo el responsable deberá fundar su respuesta y comunicar en forma electrónica su decisión al Consejo para la Transparencia y la Protección de Datos Personales. El titular podrá reclamar de esta decisión ante el Consejo para la Transparencia y la Protección de Datos Personales, aplicándose lo dispuesto en la letra a) del artículo 41[630].

La rectificación, cancelación u oposición al tratamiento de los datos se aplicará sólo respecto de los responsables a quienes se les haya formulado la solicitud. Con todo, cuando el responsable haya comunicado dichos datos a otras personas, deberá

[629] Se refiere precisamente a un procedimiento administrativo de tutela de derechos, donde el titular de datos podrá reclamar ante el Consejo cuando el responsable le haya denegado una solicitud realizada o no hubiere dado respuesta a dicha solicitud dentro del plazo legal establecido en ese artículo.

[630] Es decir, la reclamación deberá ser presentada por escrito, en formato físico o electrónico dentro del plazo de 15 días hábiles contado desde que reciba la respuesta negativa del responsable de datos o haya vencido el plazo que disponía el responsable para responder el requerimiento formulado por el titular. La reclamación deberá señalar la decisión impugnada en caso de rechazo u omisión de respuesta y acompañar todos los antecedentes en que aquella se funda e indicar un domicilio postal o una dirección correo u otro medio electrónico equivalente donde se practicarán las notificaciones.

comunicar a estas los cambios realizados en virtud de la rectificación, cancelación u oposición.
El titular podrá aportar cualquier otro antecedente que facilite la localización de los datos personales.

7. El proyecto de ley también refuerza la regla general del tratamiento de datos, en el sentido de que este es lícito cuando el tratamiento de los datos personales que le conciernen al titular se realiza con su consentimiento. Esta regla tiene excepciones que están descritas en la legislación que se propone, es decir, casos en que es lícito el tratamiento de datos personales sin el consentimiento de su titular. Entre estas hipótesis de habilitación legal se encuentran: a) Cuando los datos han sido recolectados de una fuente de acceso público; b) Cuando el tratamiento esté referido a datos relativos a obligaciones de carácter económico, financiero, bancario o comercial y se realice de conformidad con las normas previstas en la ley; c) Cuando el tratamiento sea necesario para la ejecución o el cumplimiento de una obligación legal o lo disponga la ley; d) Cuando el tratamiento de datos sea necesario para la celebración o ejecución de un contrato entre el titular y el responsable, o para la ejecución de medidas precontractuales adoptadas a solicitud del titular; e) Cuando el tratamiento sea necesario para la satisfacción de intereses legítimos del responsable o de un tercero, siempre que con ello no se afecten los derechos y libertades del titular. En todo caso, el titular podrá exigir siempre ser informado sobre el tratamiento que lo afecta y cuál es el interés legítimo en base al cual se efectúa dicho tratamiento; y f) Cuando el tratamiento de datos sea necesario para la formulación, ejercicio o defensa de un derecho ante los tribunales de justicia.

8. El precepto actualmente en discusión en el Senado también aborda las obligaciones del responsable de los datos, señalando entre otras el deber de informar y poner a disposición del titular los antecedentes que acrediten la licitud del tratamiento de datos que realiza. Igualmente, deberá entregar de manera expedita dicha información cuando le sea requerida.

Además, el responsable de datos que no tenga domicilio en Chile y que realice tratamiento de datos de personas que residan en el territorio nacional, deberá señalar y mantener actualizado y operativo un correo electrónico u otro medio de contacto idóneo para recibir comunicaciones de los titulares de datos y del Consejo para la Transparencia y la Protección de Datos Personales.

De igual forma, el responsable de datos está obligado a mantener secreto o confidencialidad acerca de los datos personales que conciernan a un titular, salvo cuando el titular los hubiere hecho manifiestamente públicos. Este deber subsiste aún después de concluida la relación con el titular. En caso de que el responsable haya realizado alguna acción sobre datos personales obtenidos de fuentes de acceso público, tales como organizarlos o clasificarlos bajo algún criterio, o combinarlos o

complementarlos con otros datos, los datos personales que resulten de dicha acción se encontrarán protegidos bajo el presente deber de secreto o confidencialidad.

9. La Ley 19.628 carecía de una definición acabada respecto a los deberes de seguridad que debían regir en el tratamiento de la información personal, limitándose a exigir "cuidar de ellos con la debida diligencia, haciéndose responsable de los daños". La propuesta legislativa actualmente en tramitación, siguiendo la línea de lo planteado en RGPD, incorpora un artículo 14 quinquies, que dispone las medidas de seguridad que debe adoptar el responsable de los datos, señalando: "El responsable de datos debe adoptar las medidas necesarias para resguardar el cumplimiento del principio de seguridad establecido en esta ley, considerando el estado actual de la técnica y los costos de aplicación, junto con la naturaleza, alcance, contexto y fines del tratamiento, así como la probabilidad de los riesgos y la gravedad de sus efectos en relación con el tipo de datos tratados. Las medidas aplicadas por el responsable deben asegurar la confidencialidad, integridad, disponibilidad y resiliencia de los sistemas de tratamiento de datos. Asimismo, deberán evitar la alteración, destrucción, pérdida, tratamiento o acceso no autorizado.

Si las bases de datos que opera el responsable tienen distintos niveles de riesgo, deberá adoptar las medidas de seguridad que correspondan al nivel más alto.
Ante la ocurrencia de un incidente de seguridad, y en caso de controversia judicial o administrativa, corresponderá al responsable acreditar la existencia y el funcionamiento de las medidas de seguridad adoptadas en base a los niveles de riesgo y a la tecnología disponible".

Como es posible advertir del articulado propuesto, lo que la legislación aún en ciernes busca, es elevar los estándares de la seguridad de la información, estableciendo mayores niveles de responsabilidad o si se quiere una responsabilidad activa en el resguardo del tratamiento de datos similar a lo que ocurre en la normativa europea.

De igual forma, lo preceptuado en el proyecto de ley hace referencia al estado actual de la técnica y costos de aplicación derivados del tratamiento de datos de carácter personal que deberá considerar el responsable de los datos, cuestión que permite vincular estas medidas de seguridad con normas de estandarización internacional tales como: las norma IS0, la 27001 sobre Seguridad de la Información[631] y la 27701 sobre Sistemas de Gestión

[631] Ver en: ISO 27001 - Software ISO 27001 de Sistemas de Gestión (isotools.org) consulta realizada el 21 de enero de 2021.

de la Información de Privacidad[632], el marco de Ciberseguridad NIST[633], o las reglas OWASP sobre los Estándares de Verificación de Seguridad de Aplicaciones Móviles[634].

El Proyecto de Ley establece el deber de reportar las brechas de seguridad por parte del responsable, debiendo informar a la Autoridad de Control de la forma más expedita posible cuáles han sido estas vulneraciones, sus posibles consecuencias, categorías de datos involucrados y un estimado de posibles afectados por dicho evento, junto con notificar cuáles serán las medidas adoptadas para mitigar el hecho y precaver futuros incidentes. Asimismo, la misma información deberá ser entregada a los titulares involucrados en caso de tratarse de información sensible, o datos de carácter económico, bancario o comercial. En efecto, el responsable y el encargado de datos deberán reportar al Consejo para la Transparencia y la Protección de Datos Personales, por los medios más expeditos posibles y sin dilaciones indebidas, las vulneraciones a las medidas de seguridad que ocasionen la destrucción, filtración, pérdida o alteración accidental o ilícita de los datos personales que trate o la comunicación o acceso no autorizados a dichos datos, cuando exista un riesgo razonable para los derechos y libertades de los titulares.

El responsable y el encargado de datos deberán registrar estas comunicaciones, describiendo la naturaleza de las vulneraciones sufridas, sus efectos, las categorías de datos y el número aproximado de titulares afectados y las medidas adoptadas para gestionarlas y precaver incidentes futuros.

De igual forma, el proyecto de manera armónica se refiere al resguardo de la información o datos personales sensibles de niños, niñas y menores de catorce años, al señalar que cuando dichas vulneraciones se refieran a datos personales sensibles, datos relativos a niños y niñas menores de catorce años o datos relativos a obligaciones de carácter económico, financiero, bancario o comercial, el responsable y el encargado de datos deberán también efectuar esta comunicación a los titulares de estos datos. Esta comunicación deberá realizarse en un lenguaje claro y sencillo, singularizando los datos afectados, las posibles consecuencias de las vulneraciones de seguridad y las medidas de solución o resguardo adoptadas. La notificación se deberá realizar a cada titular afectado y si ello no fuere posible, se realizará mediante la difusión o publicación de un aviso en un medio de comunicación social masivo y de alcance nacional[635].

---

[632] Ver en: ISO - ISO/IEC 27701:2019 - Security teniques — Extensión to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — Requirements and guidelines consulta realizada el 21 de enero de 2021.

[633] Ver en: OEA-AWS-Marco-NIST-de-Ciberseguridad-ESP.pdf (oas.org) consulta realizada el 21 de enero de 2021.

[634] Ver en: Estándar de Verificación de Seguridad en Aplicaciones 3.0.1 (owasp.org) consulta realizada el 21 de enero de 2021.

[635] Artículo 14 sexies del proyecto de ley.

10. El proyecto en primer trámite constitucional también innova respecto del tratamiento de los datos de salud, cuando estos han sido recogidos en determinados ámbitos. En efecto, queda prohibido el tratamiento y la cesión de los datos relativos a la salud y al perfil biológico de un titular y las muestras biológicas asociadas a una persona identificada o identificable, incluido el almacenamiento del material biológico, cuando los datos o muestras han sido recolectados en el ámbito laboral, educativo, deportivo, social, de seguros, de seguridad o identificación, salvo que la ley expresamente autorice su tratamiento en casos calificados.

Las excepciones para tratar datos sin el consentimiento mencionado se entienden aplicables al tratamiento de datos que no revisten el carácter especial, como los ya mencionados.

11. Actualizándose a los avances tecnológicos, la propuesta legislativa considera también dentro de los datos sensibles, el tratamiento de datos personales biométricos, que son aquellos obtenidos a partir de un tratamiento técnico específico, relativos a las características físicas, fisiológicas o conductuales de una persona que permitan o confirmen la identificación única de ella, tales como la huella digital, el iris, los rasgos de la mano o faciales y la voz.

Solo podrán tratarse estos datos cuando se cumpliere con lo dispuesto en el inciso primero del artículo 16 del proyecto de ley, esto es "cuando el titular a quien conciernen estos datos manifiesta su consentimiento en forma expresa, otorgado a través de una declaración escrita, verbal o por un medio tecnológico equivalente", y siempre que el responsable proporcione al titular la siguiente información: a) La identificación del sistema biométrico usado; b) La finalidad específica para la cual los datos recolectados por el sistema biométrico serán utilizados; c) El período durante el cual los datos biométricos serán utilizados; y d) La forma en que el titular puede ejercer sus derechos.

Los datos personales biométricos podrán tratarse sin consentimiento, en los siguientes casos:

a) Cuando este resulte indispensable para salvaguardar la vida o integridad física o psíquica del titular o de otra persona o, cuando el titular se encuentre física o jurídicamente impedido de otorgar su consentimiento. Una vez que cese el impedimento, el responsable debe informar detalladamente al titular los datos que fueron tratados y las operaciones específicas de tratamiento que fueron realizadas.

b) En casos de urgencia sanitaria legalmente decretada.

c) Cuando sean utilizados con fines históricos, estadísticos o científicos, para estudios o investigaciones que atiendan fines de interés público o vayan en beneficio de la salud humana, o para el desarrollo de productos o insumos médicos que no podrían

desarrollarse de otra manera. Los resultados de los estudios e investigaciones científicas que utilicen datos personales relativos a la salud o al perfil biológico, pueden ser publicados o difundidos libremente, debiendo previamente anonimizarse los datos que se publiquen.

d) Cuando el tratamiento de los datos sea necesario para la formulación, ejercicio o defensa de un derecho ante los tribunales de justicia o un órgano administrativo.

e) Cuando el tratamiento sea necesario para fines de medicina preventiva o laboral, evaluación de la capacidad laboral del trabajador, diagnóstico médico, prestación de asistencia o tratamiento de tipo sanitario o social, o gestión de sistemas y servicios de asistencia sanitaria y social.

f) Cuando la ley así lo permita e indique expresamente la finalidad que deberá tener dicho tratamiento.

12. El proyecto de ley también define el régimen de tratamiento de datos realizados por organismos públicos competentes en ciertas y determinadas materias, como aquellos tratamientos que se realicen con fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, incluidas las actividades de protección y prevención frente a las amenazas y riesgos contra la seguridad pública.

Aquellos en materias relacionadas directamente con la seguridad de la nación, la defensa nacional y la política exterior del país; aquellos realizados con el objeto exclusivo de atender una situación de emergencia o catástrofe, declarada de conformidad a la ley y solo mientras permanezca vigente esta declaración; aquellos que se encuentren protegidos por normas de secreto, reserva o confidencialidad, establecidas en sus respectivas leyes. Entendiéndose también comprendidos los datos que, en cumplimiento de una obligación legal, los órganos públicos deban ceder a otro órgano público o a terceros, debiendo en tal caso el receptor tratarlos manteniendo la misma obligación de secreto, reserva o confidencialidad.

Los órganos públicos correspondientes podrán tratar, ceder y comunicar datos personales de forma lícita, siempre y cuando se realice para el cumplimiento de sus funciones legales, dentro del ámbito de sus competencias y respetando las garantías fundamentales establecidas en el artículo 19 N° 4 de la Constitución Política de la República y los principios para el tratamiento de datos personales.

Con el objeto de realizar los tratamientos, cesiones y comunicaciones de datos para resguardar la seguridad pública, la seguridad de la Nación, la defensa nacional y la política exterior del país, o atender una situación de emergencia o catástrofe, los

órganos públicos y sus autoridades estarán obligadas a intercambiar información y proporcionar los datos personales que les sean requeridos para estos fines, siempre que se refieran a tratamientos que se realicen con una finalidad específica autorizada por ley o, cuando esto no sea posible, el requerimiento sea una medida necesaria y proporcional.

El Consejo para la Transparencia y la Protección de Datos podrá, oyendo previamente a los órganos competentes, dictar instrucciones para especificar la forma de aplicar las referidas garantías y principios a los casos mencionados, de manera de asegurar su resguardo y permitir el debido cumplimiento de las funciones legales de los órganos correspondientes.

13. El proyecto de ley también se refiere a los datos personales relacionados con las condenas de infracciones penales, civiles, administrativas o disciplinarias en el sentido de que no podrán comunicarse o hacerse públicos una vez prescrita la acción penal, civil, administrativa o disciplinaria respectiva, o una vez que se haya cumplido o prescrito la pena o la sanción impuesta, lo que deberá ser declarado o constatado por la autoridad competente.

Lo anterior es, sin perjuicio de la incorporación, mantenimiento y consulta de esta información en los registros que llevan los órganos públicos por expresa disposición de la ley, en la forma y por el tiempo previsto en la ley que establece la obligación específica correspondiente. Las personas que se desempeñen en los órganos públicos están obligadas a guardar secreto respecto de esta información, la que deberá ser mantenida como información reservada.

Además, los datos personales relativos a la comisión y sanción de infracciones penales revisten carácter reservado y, salvo las disposiciones legales que autorizan su tratamiento, no podrán ser comunicados o cedidos a terceras personas por los organismos públicos que los posean.

14. El título V del proyecto de ley se refiere a la transferencia internacional de datos personales, estableciéndose los requisitos necesarios para que dicho tratamiento sea lícito, ya sea que se realice a una persona, entidad u organización pública o privada, sujeta al ordenamiento jurídico de un país que proporcione niveles adecuados de protección de datos personales. El nivel adecuado de protección de datos se cumple cuando el referido país en su ordenamiento jurídico cumple con estándares similares o superiores a los establecidos en el proyecto de ley, lo que será determinado por el Consejo para la Transparencia y la Protección de Datos Personales considerando entre otros aspectos: a) El establecimiento de principios que rigen el tratamiento de los datos personales; b) La existencia de normas que reconozcan y garanticen los derechos de los titulares de datos y la existencia de una autoridad pública jurisdiccional o administrativa de control o tutela; c) La imposición de obligaciones de información y

seguridad a los responsables del tratamiento de los datos; y d) La determinación de responsabilidades en caso de infracciones.

Cuando no se verifique ninguna de las circunstancias señaladas, el Consejo para la Transparencia y la Protección de Datos Personales podrá autorizar, mediante resolución fundada, la transferencia internacional de datos siempre que el transmisor y el receptor de los datos otorguen las garantías adecuadas en relación con la protección de los derechos de las personas que son titulares de estos datos y la seguridad de la información transferida.

Finalmente, corresponderá al responsable de datos que efectuó la transferencia internacional de datos, acreditar que esta se practicó de conformidad a las reglas establecidas en esta ley.

15. El título VI del proyecto de ley, entre los artículos 30 al 32 se refiere a la consagración como Autoridad de Control en protección de datos, como ya se ha señalado, al Consejo para la Transparencia, que ahora pasará a denominarse Consejo para la Transparencia y la Protección de Datos. En otro apartado de este trabajo se profundizará en su configuración y las principales funciones y atribuciones que le son asignadas, así como la conveniencia o no de que sea esta entidad, ya existente en la estructura administrativa chilena la que se configure como responsable de la protección de datos personales.

16. El proyecto de ley se refiere a las infracciones y sanciones derivadas del incumplimiento de sus disposiciones. Sobre las infracciones cometidas por los responsables de datos a los principios, derechos y obligaciones establecidos en el proyecto de ley, se califican, atendida su gravedad, en leves, graves y gravísimas.

Por ejemplo, es una infracción leve el carecer de la individualización del domicilio postal, correo o medios electrónicos equivalentes que permita comunicarse con el responsable de datos o su representante legal, actualizado y operativo, a través del cual los titulares de datos puedan dirigir sus comunicaciones o ejercer sus derechos. A su vez son infracciones graves, por ejemplo: a) Comunicar o ceder datos personales, sin el consentimiento del titular, en los casos en que dicho consentimiento sea necesario, o comunicar o ceder los datos para un fin distinto del autorizado; o b) Tratar datos personales inexactos, incompletos o desactualizados en relación con los fines del tratamiento, salvo que la actualización de estos datos corresponda al titular en virtud de la ley o el contrato.

Entre las infracciones gravísimas se pueden señalar: a) Efectuar tratamiento de datos personales en forma fraudulenta; b) Destinar maliciosamente los datos personales a una finalidad distinta de la consentida por el titular o prevista en la ley que autoriza su tratamiento; c) Comunicar o ceder, a sabiendas, información no veraz, incompleta,

inexacta o desactualizada sobre el titular de datos; d) Vulnerar el deber de secreto o confidencialidad sobre los datos personales sensibles y datos personales relativos a la comisión y sanción de infracciones penales, civiles, administrativas y disciplinarias; o e) Tratar, comunicar o ceder, a sabiendas, datos personales sensibles o datos personales de niños, niñas y adolescentes, en contravención a las normas de esta ley.

Sobre las sanciones el proyecto avanza también de manera significativa, en el sentido de incrementar sustancialmente su monto. Lo hace a través de la Unidad Tributaria Mensual o UTM[636], 1 UTM a diciembre del año 2020 equivalía a cincuenta y un mil veintinueve pesos ($ 51.029), es decir 57,06 euros. Las sanciones a las infracciones en que incurran los responsables de datos serán las siguientes: a) Las infracciones leves serán sancionadas con amonestación escrita o multa de 1 a 100 unidades tributarias mensuales; b) Las infracciones graves serán sancionadas con multa de 101 a 5.000 unidades tributarias mensuales; y c) Las infracciones gravísimas serán sancionadas con multa de 5.001 a 10.000 unidades tributarias mensuales.

17. El proyecto de ley además reestructura todo el procedimiento de reclamación por la vía administrativa, en caso de tutela de derechos o por infracción a la ley, ante el Consejo para la Transparencia y la Protección de Datos Personales, dichos procedimientos deberán tener una duración máxima de seis meses, en caso de incumplimiento de peste plazo se podrá seguir la vía judicial. Como por la vía jurisdiccional ante la Corte de Apelaciones de Santiago o la del domicilio del reclamante a su elección, acción que se denomina reclamo de ilegalidad.

18. En relación con el régimen de responsabilidad, el proyecto de ley distingue entre la responsabilidad administrativa del órgano público, de la autoridad o jefe de servicio y del funcionario, los cuales podrán infringir las disposiciones del proyecto de ley tipificándose como infracciones leves, graves y gravísimas, conductas que serán sancionadas con una multa de veinte por ciento a cincuenta por ciento de la remuneración mensual del jefe superior del órgano público infractor. La cuantía de la multa se determinará considerando la gravedad de la infracción, la naturaleza de los datos tratados y el número de titulares afectados, así como las circunstancias que atenúan la responsabilidad del infractor.

Si el órgano público persiste en la infracción, se le aplicará al jefe superior del órgano público el duplo de la sanción originalmente impuesta y la suspensión en el cargo por un lapso de cinco días. Tratándose de datos personales sensibles la multa será del 50%

[636] La unidad tributaria mensual es una unidad de cuenta usada en Chile para efectos tributarios y de multas, actualizada según la inflación. Fue creada el 31 de diciembre de 1974 mediante el artículo 8.º del decreto ley N°830. Inicialmente, fue una medida tributaria usada por el Servicio de Impuestos Internos.

de la remuneración mensual del jefe superior del órgano público y procederá la suspensión en el cargo de hasta treinta días[637].
Las infracciones en que incurra un órgano público en el tratamiento de los datos personales serán determinadas por el Consejo para la Transparencia y la Protección de Datos Personales de acuerdo con el procedimiento establecido para las infracciones a las disposiciones del proyecto de ley.

Respecto de la responsabilidad del funcionario público infractor, el proyecto de ley establece que si en el procedimiento administrativo correspondiente se determina que existen responsabilidades individuales de uno o más funcionarios del órgano público, la Contraloría General de la República, a petición del Consejo para la Transparencia y la Protección de Datos Personales, iniciará una investigación sumaria[638] para determinar las responsabilidades de dichos funcionarios o lo hará en el procedimiento administrativo ya iniciado, en su caso. Las sanciones a los funcionarios infractores serán determinadas de conformidad a lo dispuesto en el Estatuto Administrativo.

En caso de que el procedimiento administrativo correspondiente determine que cualquiera de los funcionarios involucrados es responsable de alguna de las

[637] Sobre las sanciones a las autoridades o jefaturas de los servicios públicos, el proyecto de ley sigue la misma línea que la ley 20.285 sobre acceso a la información pública, que entre los artículos 45 y 47 también sanciona con un porcentaje de disminución de su remuneración mensual a la respectiva jefatura. "Artículo 45.- La autoridad o jefatura o jefe superior del órgano o servicio de la Administración del Estado, requerido, que hubiere denegado infundadamente el acceso a la información, contraviniendo, así, lo dispuesto en el artículo 16, será sancionado con multa de 20% a 50% de su remuneración; Artículo 46.- La no entrega oportuna de la información en la forma decretada, una vez que ha sido ordenada por resolución a firme, será sancionada con multa de 20% a 50% de la remuneración correspondiente. Si la autoridad o jefatura o jefe superior del órgano o servicio de la Administración del Estado, requerido, persistiere en su actitud, se le aplicará el duplo de la sanción indicada y la suspensión en el cargo por un lapso de cinco días; y Artículo 47.- El incumplimiento injustificado de las normas sobre transparencia activa se sancionará con multa de 20% a 50% de las remuneraciones del infractor".

[638] Es un procedimiento administrativo disciplinario establecido en el Estatuto Administrativo, Ley N°18.834, al que hace referencia el artículo 120 al señalar: "Si el jefe superior de la institución, el Secretario Regional Ministerial o el Director Regional de servicios nacionales desconcentrados, según corresponda, estimare que los hechos son susceptibles de ser sancionados con una medida disciplinaria o en el caso de disponerlo expresamente la ley, ordenará mediante resolución la instrucción de una investigación sumaria, la cual tendrá por objeto verificar la existencia de los hechos, y la individualización de los responsables y su participación, si los hubiere, designando para tal efecto a un funcionario que actuará como investigador.

Las notificaciones que se realicen durante la investigación sumaria deberán hacerse personalmente. Si el funcionario no fuere habido por dos días consecutivos en su domicilio o en su lugar de trabajo, se lo notificará por carta certificada, de lo cual deberá dejarse constancia. En ambos casos se deberá dejar copia íntegra de la resolución respectiva. En esta última circunstancia, el funcionario se entenderá notificado cumplidos tres días desde que la carta haya sido despachada.

El procedimiento será fundamentalmente verbal y de lo actuado se levantará un acta general que firmarán los que hayan declarado, sin perjuicio de agregar los documentos probatorios que correspondan, no pudiendo exceder la investigación el plazo de cinco días. Al término del señalado plazo se formularán cargos, si procedieren, debiendo el afectado responder los mismos en un plazo de dos días, a contar de la fecha de notificación de éstos…

infracciones gravísimas, esta conducta se considerará una contravención grave a la probidad administrativa.

Además de lo señalado, el proyecto de ley asigna a los funcionarios públicos el deber de reserva y confidencialidad; en efecto, aquellos que traten datos personales y especialmente, cuando se refieran a datos personales sensibles o datos relativos a la comisión y sanción de infracciones penales, civiles, administrativas y disciplinarias, deben guardar secreto o confidencialidad respecto de la información que tomen conocimiento en el ejercicio de sus cargos y abstenerse de usar dicha información con una finalidad distinta de la que corresponda a las funciones legales del órgano público respectivo[639] o utilizarla en beneficio propio o de terceros, en caso contrario el proyecto de ley establece que se configura una vulneración grave al principio de probidad administrativa, sin perjuicio de las demás sanciones y responsabilidades que procedan.

También el responsable de los datos estará afecto a un régimen de responsabilidad civil, por cuanto deberá indemnizar el daño patrimonial y extra patrimonial (daño moral) que cause al o los titulares, cuando en sus operaciones de tratamiento de datos infrinja los principios, derechos y obligaciones establecidos y les cause perjuicio. Lo anterior no obsta al ejercicio de los demás derechos que se concedan al o los titulares de datos. Esta acción indemnizatoria podrá interponerse una vez ejecutoriada la resolución que resolvió favorablemente el reclamo interpuesto ante el Consejo para la Transparencia y la Protección de Datos Personales o la sentencia se encuentre firme y ejecutoriada, en caso de haber presentado un reclamo de ilegalidad y se tramitará de conformidad a las normas del procedimiento sumario establecidas en el artículo 680 y siguientes del Código de Procedimiento Civil chileno[640].

19. Un aspecto novedoso en la legislación que se discute en el Senado es el que dice relación con el establecimiento de sistemas de prevención para el adecuado tratamiento de datos de carácter personal. Así, el proyecto en discusión dispone un "Modelo de prevención de infracciones", que consiste en que los responsables de datos podrán voluntariamente adoptar mecanismos que configuran dicho modelo, los cuales son: a) Designación de un encargado de prevención o delegado de protección de datos personales. Los órganos públicos que establezcan un encargado de prevención o delegado de protección de datos personales deberán designar para ello a un funcionario

[639] Esto por cuanto el proyecto también considera cuando en cumplimiento de una obligación legal un órgano público comunica o cede a otro órgano público datos protegidos por normas de secreto o confidencialidad, el organismo público receptor y sus funcionarios, deberán tratarlos manteniendo la misma obligación de secreto o confidencialidad.

[640] El proyecto de ley también dispone que las acciones civiles que deriven de una infracción prescribirán en el plazo de cinco años, contados desde que se encuentre ejecutoriada la resolución administrativa o la sentencia judicial, según sea el caso, que imponga la multa respectiva.

de la dotación vigente del respectivo organismo; y b) Adopción de un programa de cumplimiento o de prevención de infracciones.

El Consejo para la Transparencia y la Protección de Datos Personales será la entidad encargada de certificar que el modelo de prevención de infracciones y el programa de cumplimiento reúna los requisitos y elementos establecidos en la ley y su respectivo reglamento[641], además será la entidad encargada de supervisarlos y creará un registro público en que consten las entidades que posean una certificación y aquellas cuya certificación haya sido revocada.

Hacia una Autoridad de Control para la Protección de Datos para Chile

Un elemento trascendental en la discusión legislativa para una nueva institucionalidad para la protección de datos en Chile es la configuración de una Autoridad de Control. Si bien en el Capítulo IV de esta investigación se abordaron las principales características que configuran una entidad de esta naturaleza y se examinó la experiencia comparada en la materia, ahora corresponde revisar cómo el actual proyecto de ley chileno, en discusión en primer trámite constitucional en el Senado, estructura una entidad que no solo regule sino que además promueva la protección de datos de carácter personal y sintonice con la regulación comparada, principalmente la europea, que consagra una Autoridad de Control en cada país miembro de la Unión con amplias competencias, funciones y poderes.

El proyecto busca la creación de una nueva institucionalidad de control, encargada de velar por el efectivo cumplimiento de la regulación en protección de datos, con funciones normativas, fiscalizadoras y sancionatorias. Por consiguiente, este aspecto ha sido uno de los principales puntos de discusión durante su tramitación, especialmente respecto a la naturaleza y rol del organismo en ciernes.

A continuación, se revisará la evolución que en los boletines refundidos N°11.144-07 y 11.092-07 ha tenido la regulación de una autoridad de control, para luego hacer un análisis de las fortalezas y debilidades que tendría el adoptar uno u otro modelo, esto es, optar por la creación de una Autoridad para la Protección de Datos o radicar esa atribución en otra entidad ya existente como el Consejo para la Transparencia.

En las siguientes líneas se analizarán los principales alcances de la discusión Legislativa relacionada con el establecimiento de una autoridad de control en materia de protección de datos, desarrollada fundamentalmente en la Comisión de Legislación, Justicia y Reglamento del Senado.

[641] Un reglamento expedido por el Ministerio de Hacienda y suscrito por el Ministro Secretario General de la Presidencia y por el Ministro de Economía, Fomento y Turismo establecerá los requisitos, modalidades y procedimientos para la implementación, certificación, registro y supervisión de los modelos de prevención de infracciones y los programas de cumplimiento.

La Agencia de Protección de Datos

El Proyecto, en una primera etapa, creaba una entidad integrante de la estructura administrativa a cargo de la protección de Datos Personales como un organismo público, de carácter técnico, descentralizado, con personalidad jurídica y patrimonio propio, encargado de velar por el cumplimiento de la normativa relativa al tratamiento de los datos personales.

En efecto, en sus inicios el proyecto planteaba el crear una autoridad de control encargada de velar por la protección de los derechos y libertades de las personas titulares de datos. Esta unidad estaría dotada de facultades para regular, supervisar, fiscalizar y en última instancia, sancionar los incumplimientos de la ley.

Para alcanzar este objetivo se propone crear una institución especializada y de carácter técnico, denominada "Agencia de Protección de Datos Personales", cuyo objetivo es velar y fiscalizar el cumplimiento de esta normativa. Ella se relacionaría con el Presidente de la República a través del Ministerio de Hacienda estando afecta al Sistema de Alta Dirección Pública.

En el transcurso de la discusión legislativa, según consta en el boletín N°11.092-07, el día 14 de marzo de 2017, se dio cuenta en el Senado del Oficio N° 34, del 13 de marzo de 2017, de la Excma. Corte Suprema en que comunica su parecer sobre esta iniciativa. En dicho informe se señala, en lo esencial en lo referente a la autoridad de control hasta esa fecha propuesta, lo siguiente: "Que otro asunto de carácter general, consiste en que el proyecto no crea bases institucionales y orgánicas que rijan el sistema de protección de datos personales. Esta carencia del proyecto es explicada en la moción en las limitaciones de las facultades de los senadores en materia de iniciativa legal, que les habría impedido corregir el que parece ser uno de los defectos más importantes del sistema, a saber, la inexistencia de una institucionalidad adecuada en estas materias".

Respecto de este punto, cabe observar que habitualmente las normativas que regulan el derecho a la protección de los datos personales van acompañadas del establecimiento de autoridades encargadas del control o supervisión de su cumplimiento. En general, a esta institucionalidad se le entregan facultades que implican, a lo menos, contar con total independencia de los poderes políticos en el ejercicio de sus funciones y estar dotadas de atribuciones que permitan la supervisión adecuada de las normas específicas de protección de datos. En general los países que cuentan con autoridades de control con las prerrogativas señaladas cumplen con un "nivel adecuado de protección", agregando la Corte Suprema sobre este punto que: "Debe tenerse en especial consideración la incorporación de Chile a la OCDE. El 7 de Mayo del 2010, Chile firmó el Convenio de Adhesión a la Organización para la Cooperación y el Desarrollo Económico (OCDE) y compromete plena dedicación a la consecución de los objetivos fundamentales de dicha organización. En relación con el derecho de la protección de los datos personales, la OCDE ha emitido una serie de recomendaciones, entre las que destaca la Recomendación sobre Protección de la Privacidad y Flujo Transfronterizo de Datos Personales. Las directrices, en cuanto a la implementación de medidas internas, establecen que los países miembros deben adoptar una legislación nacional adecuada, impulsar y apoyar la autorregulación ya sea mediante códigos de conducta o de otro modo; brindar los medios razonables para que los individuos ejerzan sus derechos; sancionar adecuadamente y ofrecer soluciones en caso de fallos, con el fin de cumplir las medidas de implantación y asegurar que no haya discriminación desleal hacia el sujeto de los datos".

Y luego señala que: “En tal sentido, corresponde advertir que tanto el diseño institucional previsto por la ley vigente como por el proyecto actualmente en análisis, a pesar de propiciar la introducción de nuevos principios, derechos y prerrogativas, no cumplirían con los estándares de ‘nivel adecuado de protección’ que en materia de datos exige la comunidad internacional”.

Sobre el ausencia de una autoridad de control en materia de protección de datos personales se refirió también el Subsecretario del Ministerio de Hacienda de la época señor Alejandro Micco, que durante su exposición en la Comisión de Constitución, Legislación, Justicia y Reglamento del Senado señaló que: “Tanto de la experiencia comparada como de las recomendaciones de la OCDE a Chile, se desprende que nuestro país no cuenta con un organismo que supervise el correcto tratamiento y protección de los datos personales. Agregó que tanto el informe del Consejo para la Transparencia, como el de la Corte Suprema sobre el último proyecto de ley de protección de datos personales coinciden en la falta de una nueva institucionalidad.

Sostuvo que en la evaluación de la ley N° 19.628 sobre Protección de la Vida Privada de la Cámara de Diputados, se concluye que la legislación chilena requiere de una autoridad administrativa de control independiente.

En esta materia, expresó que a nivel mundial existe una serie de formas que adopta la institucionalidad para la protección de los datos. Consignó que la tendencia a nivel mundial consiste en contar con una institucionalidad exclusiva, separada de la de la transparencia. Aseveró que es necesario analizar cómo interactúa el derecho de proteger los datos personales con la transparencia y se preguntó si estas debían estar bajo el alero de distintos organismos.

Constató que la mayoría de los países cuentan con instituciones que funcionan de manera independiente. Para ello, puntualizó, hay diversas razones, una de ellas es que estamos frente a dos derechos que pueden ser contradictorios.

Lo anterior, explicó, motivó la separación de ambas institucionalidades en el presente proyecto de ley. Agregó que en la iniciativa se crea la Agencia de Protección de Datos Personales, la que gozará de cierto nivel de autonomía.

Asimismo, afirmó que se crea un régimen general de cumplimiento de la ley que tiene un procedimiento administrativo por infracción a la ley. Manifestó que este se puede iniciar a petición de parte o de oficio. Posterior a ello, la Agencia presentará la formulación de cargos contra el responsable de los datos y este último tiene diez días de plazo para presentar los descargos. En caso de que existan hechos sustanciales, pertinentes y controvertidos se abre un término probatorio de siete días. Agregó que la Agencia deberá pronunciarse sobre cada uno de los aspectos conocidos en el expediente y frente a esa resolución se puede interponer recurso de reposición dentro del plazo de cinco días.

Detalló que de la resolución de la Agencia se podrá presentar una reclamación judicial. Señaló que la persona natural o jurídica que se vea afectada por una resolución final de la Agencia de Protección de Datos Personales podrá deducir un reclamo de ilegalidad a la Corte de Apelaciones respectiva. La Corte requerirá informe a la Agencia, concediéndole un plazo de diez días y el mencionado tribunal podrá abrir un término probatorio si lo considera necesario. Añadió que vencido este plazo se ordenará traer los autos en relación. Subrayó que la vista de

esta causa gozará de preferencia. Recalcó que la Corte puede confirmar la decisión de la Agencia u ordenar que ésta rectifique su resolución"[642].

El Subsecretario Micco finalizó su exposición señalando que entre los objetivos del proyecto de ley está el "Contar con una autoridad de control de carácter técnico y una institucionalidad pública que asuma los desafíos regulatorios y de fiscalización en materia de protección de las personas y el tratamiento de los datos personales.

Como conclusión a lo ya expresado, manifestó que el actual marco regulatorio es insuficiente frente a los cambios tecnológicos, económicos y culturales de las últimas décadas; falta una autoridad de control que vele por la correcta aplicación de la ley y debe cumplirse con los compromisos adquiridos internacionalmente. Enfatizó que existen tres principios fundamentales que deben ser cautelados, a saber: la transparencia, la libre circulación de la información y la protección de la vida privada.

Concluyó su intervención haciendo referencia al informe financiero. Consignó que la iniciativa se estima tendrá un mayor gasto fiscal en régimen de $ 1.428.876 miles, a partir del segundo año de vigencia de la ley, asociado a la creación de la Agencia de Protección de Datos Personales"[643].

También durante la discusión legislativa concurren a la Comisión los representantes de la época del Consejo para la Transparencia a saber su presidente señor José Luis Santa María y la Directora Jurídica del Consejo para la Transparencia, señora Andrea Ruiz. Sobre la institucionalidad que se propone el señor Santa María planteó resumidamente que la autoridad de control debe alcanzar estándares internacionales de independencia para cumplir adecuadamente su rol. Agregó que según el estándar europeo la dirección de una institución de esta naturaleza no debe quedar sometida a instrucciones o influencias externas, directas o indirectas[644].

A su turno la directora jurídica del Consejo para la Transparencia sobre esta materia señalo "que el proyecto de ley del Ejecutivo crea una autoridad de control, porque es esencial que exista un ente garante de los derechos de los ciudadanos, que fiscalice y sanciones cuando corresponda. Consideró que ambos proyectos pueden ser mejorados en diversos aspectos técnicos. Señaló que el Consejo para la Transparencia, desde su creación, ha aplicado la Ley sobre Protección de la Vida Privada, además de la Ley sobre Acceso a la Información Pública. Reconoció que lo han hecho con aciertos y desaciertos, porque no es fácil aplicar una norma tan antigua a las nuevas realidades"[645]. Agregando a continuación que "la Agencia de

---

[642] Primer Informe de la Comisión de Constitución, Legislación, Justicia y Reglamento recaído en el proyecto de ley, en primer trámite constitucional, que regula la protección y el tratamiento de los datos personales y crea la Agencia de Protección de Datos Personales. Boletines N$^{os.}$ 11.092-07 y 11.144 -07, refundidos, pp. 54 y 55.

[643] Primer Informe de la Comisión de Constitución, Legislación, Justicia y Reglamento recaído en el proyecto de ley, en primer trámite constitucional, que regula la protección y el tratamiento de los datos personales y crea la Agencia de Protección de Datos Personales. Boletines N$^{os.}$ 11.092-07 y 11.144 -07, refundidos, p. 58.

[644] Primer Informe de la Comisión de Constitución, Legislación, Justicia y Reglamento recaído en el proyecto de ley, en primer trámite constitucional, que regula la protección y el tratamiento de los datos personales y crea la Agencia de Protección de Datos Personales. Boletines N$^{os.}$ 11.092-07 y 11.144 -07, refundidos, p. 71.

[645] Primer Informe de la Comisión de Constitución, Legislación, Justicia y Reglamento recaído en el proyecto de ley, en primer trámite constitucional, que regula la protección y el tratamiento de los datos personales y crea la Agencia de Protección de Datos Personales. Boletines N$^{os.}$ 11.092-07 y 11.144 -07, refundidos, p. 72.

Protección de Datos que se crea solo puede conocer de los procedimientos de reclamo del sector privado y no del público. Añadió que el ciudadano que se ve enfrentado a un órgano de la Administración del Estado, debe recurrir de ilegalidad ante la Corte de Apelaciones respectiva, situación que tiene un costo que no todos pueden asumir.

En cuanto a la naturaleza de la autoridad de control, señaló que el Consejo para la Transparencia estima que ella debe ser acorde a los estándares internacionales, y éstos exigen que ella tenga independencia para el cumplimiento de sus funciones.

Agregó que el estándar europeo exige que la dirección de este tipo de instituciones no puede ser susceptible de instrucciones o influencias internas o externas, directas o indirectas. Es decir, la autoridad debe tener la suficiente capacidad para resolver con independencia los problemas que se le presentan. Precisó que la mencionada independencia ayudaría a superar la asimetría descrita entre el sector público y privado"[646].

Avanzando en la discusión legislativa uno de los senadores de la comisión, específicamente, el Senador Hernán Larraín planteó un elemento que será trascendental en el devenir del proyecto de ley. Sostiene el Senador que la Agencia de Protección de Datos debe ser autónoma e independiente y con un gobierno corporativo adecuado.

Aseveró que "el hecho de que sea un órgano adscrito al Ministerio de Hacienda le produce una inquietud mayor, porque entregarle a un Ministerio tan potente, que tiene una ocupación central, le produce una sensación equívoca. Se preguntó por qué toda la información relacionada con la protección de datos tendría que estar bajo el alero de un ministerio. Lo anterior, argumentó, alimenta la necesidad de elaborar un proyecto que garantice a los chilenos que sus datos personales estarán protegidos por una organización autónoma e independiente de todo organismo público.

Remarcó que así ocurre en el derecho comparado. Indicó que probablemente en sus inicios las agencias se adscribían a un Ministerio, pero ello ya no corresponde al estándar actual"[647].

Enfatizó que la autonomía de la Agencia constituye un capítulo central, preguntándose si la Agencia de Protección de Datos podría estar bajo el mismo alero de aquella encargada de la transparencia. Explicó que esa medida parecía razonable ejemplificando con el caso de Canadá, que bajo una misma institución están las dos agencias, pero operan en Salas especializadas. Añadió que están dotadas de un órgano superior que permite buscar la unidad de criterio.

Manifestó que el acceso a la información pública tiene un límite en la intimidad de los datos personales, explicando que a su juicio son dos caras de una misma moneda, por lo que abogó para que en esta materia haya una mirada común en la Comisión".

Más adelante el Senador Larraín agrega que es partidario que la Agencia esté bajo el alero del Consejo para la Transparencia, ya que las decisiones entre ambos no deben ser contradictorias,

---

[646] Primer Informe de la Comisión de Constitución, Legislación, Justicia y Reglamento recaído en el proyecto de ley, en primer trámite constitucional, que regula la protección y el tratamiento de los datos personales y crea la Agencia de Protección de Datos Personales. Boletines N$^{os.}$ 11.092-07 y 11.144 -07, refundidos, p. 73.

[647] Primer Informe de la Comisión de Constitución, Legislación, Justicia y Reglamento recaído en el proyecto de ley, en primer trámite constitucional, que regula la protección y el tratamiento de los datos personales y crea la Agencia de Protección de Datos Personales. Boletines N$^{os.}$ 11.092-07 y 11.144 -07, refundidos, p.83.

porque si bien regulan aspectos distintos, finalmente ambos se vinculan con la protección y el acceso a la información. Reiteró que esto constituye un tema central del proyecto, haciendo un llamado al Ejecutivo para que se haga cargo de él[648].

Según se desprende de las páginas 85 y 86 del Primer informe de la Comisión se produjo un arduo intercambio de opinión sobre dónde debía estar radicada la autoridad de control en materia de protección de datos y si esta debía o no tener carácter autónomo. En este sentido la Subsecretaria de Evaluación Social de la época, señora Heidi Berner, invitada a la Comisión, manifestó que "siempre se piensa que la mejor forma en que se resguardan los datos personales es mediante un organismo autónomo. Agregó que la discusión desde el Ejecutivo consistió en plantearse si se necesitaba un organismo autónomo o uno que técnicamente fuera independiente. Sostuvo que ella es partidaria de esto último. Hizo presente que la mencionada independencia técnica se puede llevar a cabo cuando la normativa es suficientemente clara".

A su turno, la Coordinadora de Finanzas Internacionales y Mercado de Capitales del Ministerio de Hacienda, señora Bernardita Piedrabuena justificó la existencia de la Agencia de Protección de Datos Personales en el Ministerio de Hacienda, señalando que revisaron la legislación comparada y detectaron que no existe un patrón definido. Hizo presente que en la OCDE existen muchos países en que la Agencia depende del Ejecutivo. Por lo tanto, la definición de esta dependerá de la legalidad y la cultura del país. Enfatizó que en el proyecto se opta por el Ministerio de Hacienda, por razones de eficacia y eficiencia reguladora, es decir, en dicha Cartera la Agencia tendrá un poder suficiente para hacer valer el cumplimiento de la ley.

Posteriormente el Senador Larraín sostuvo que originalmente no había claridad respecto a dónde ubicar a la mencionada Agencia, pero el debate tal cual ha evolucionado avanza hacia órganos autónomos. Subrayó que si el Ejecutivo está tan seguro de la independencia técnica debiese dar el paso de dotarla del estatus jurídico que tienen muchas instituciones en Chile. Dio el ejemplo del Banco Central, indicando que siendo autónomo tiene vinculaciones con el Gobierno, a través del Ministerio de Hacienda.

Avanzada la discusión en la Comisión, el Senador Larraín se mostró partidario de contar con un organismo colegiado como Autoridad de Control y propuso que las labores de protección de datos personales recaigan en el Consejo para la Transparencia, el que a su juicio ha logrado aplicar una legislación nueva, en un ámbito donde la cultura del secreto estaba instalada, haciendo transformaciones muy profundas. Subrayó que ha sido capaz de supervisar y llevar adelante el proceso generando opinión, investigación y estudio, y que lo mismo podría hacer en materia de protección de datos de carácter personal.

---

[648] Sobre lo señalado por el Senador Larraín la directora jurídica del Consejo para la Transparencia agrega que considera relevante que la Agencia tenga una autonomía técnica. Declaró que el hecho de tener una Agencia de Protección de Datos y un Consejo para la Transparencia podría implicar que los dos órganos terminen transformando sus egos institucionales en sus decisiones y se termine discutiendo todo en las Cortes de Apelaciones, es decir, lo que sea público o reservado en virtud de la protección de datos termine siendo resuelto por los tribunales de justicia. Ver página 84 del Primer Informe de la Comisión de Constitución, Legislación, Justicia y Reglamento recaído en el proyecto de ley, en primer trámite constitucional, que regula la protección y el tratamiento de los datos personales y crea la Agencia de Protección de Datos Personales. Boletines N$^{os.}$ 11.092-07 y 11.144 -07, refundidos.

En una nueva intervención del presidente del Consejo para la Transparencia, señor José Luis Santa María, señala que el Consejo que tiene el honor de presidir, puede hacerse cargo de la Agencia de Protección de Datos, tal como ocurre en Canadá, mediante dos Salas especializadas.

Como es posible de apreciar del análisis de la discusión, según se desprende de su Primer Informe, se colige como una opinión generalizada entre los expositores e intervinientes la importancia de avanzar desde el punto de vista institucional en la estructuración de una entidad independiente, ello por varios aspectos a considerar. En primer lugar, porque su carácter independiente no solo disminuye la influencia del gobierno en las decisiones de dicha autoridad, sino que, en caso contrario se dificulta la evaluación de su desempeño en materias regulatorias. Por ejemplo, una entidad reguladora encargada tanto de fijar tarifas como de establecer políticas públicas de desarrollo para un sector determinado tendría incentivos a fijar tarifas mayores a lo socialmente conveniente, para permitir, por ejemplo, la modernización de tal sector. Si el organismo regulador tiene dependencia del Ejecutivo, su responsabilidad pasa a ser política más que técnica por lo que, siguiendo con el ejemplo, los criterios para la determinación de las tarifas pueden no ser motivados exclusivamente por criterios de eficiencia.

En definitiva, una agencia reguladora independiente y autónoma facilita la asignación de responsabilidades específicas y el proceso de control de gestión y medición de su desempeño.

La experiencia comparada muestra que la eficacia de cualquier legislación de protección de datos personales radica en su autoridad de control y esa eficacia está indisolublemente vinculada a su carácter independiente, tanto desde la perspectiva política como desde la perspectiva técnica. Para ello resulta fundamental además que la autoridad de control en protección de datos tenga estabilidad institucional en el desarrollo de su gestión, para evitar o disminuir las presiones que provienen desde el mercado y también desde el tratamiento de datos del Gobierno. Esta estabilidad se afecta y disminuye radicando a dicha autoridad bajo la supervigilancia del Presidente de la República a través del Ministerio de Hacienda aun cuando el nombramiento de esta está determinado por el sistema de alta dirección pública, que en la práctica chilena ha demostrado que en los ciclos de cambio de gobierno renuncian casi todas las autoridades que han sido nombradas mediante ese sistema[649].

Una perspectiva interesante sobre este tema la entregó la Directora Ejecutiva de la Fundación Datos Protegidos, señora Romina Garrido, quien planteó que, a la autoridad de control en materia de protección de datos personales, con el objetivo de darle estabilidad, se le podría aplicar un régimen similar al nombramiento del Fiscal Nacional Económico. En este sentido señaló que este es designado por el Presidente de la República bajo el sistema de Alta Dirección Pública y solo puede ser removido y sancionado, según proponga la Contraloría General de la República, previo sumario instruido por esta, ejerciendo su cargo por cuatro años, renovables por una sola vez.

Con relación al nombramiento, esta autoridad no puede responder a consideraciones político-partidistas, ella debe ser independiente. Añadió que debe tener un mandato y duración definida.

[649] Solo en Nicaragua la Autoridad de Control en la experiencia comparada depende del Ministerio de Hacienda, este diseño no ha traído resultados positivos en el empoderamiento y capacidad de fiscalización de dicha entidad.

Debe ser inamovible en el tiempo para asegurar su independencia y las causales para remoción deben estar previamente definidas en la ley.

La señora Garrido planteo además que "el proyecto de ley señala que los organismos públicos quedan exentos del régimen fiscalizador y sancionatorio de la Agencia de Protección Datos Personales. Recalcó que las personas que se sientan afectadas por un tratamiento de datos por el sector público tendrán que acudir a la Corte de Apelaciones respectiva. Lo que muestra, a su juicio, que estamos ante una Agencia que no está al nivel de los otros organismos públicos y ello desincentiva a que las personas puedan denunciar malas prácticas que provengan de las entidades públicas, lo que debe ser corregido durante la tramitación legislativa".

Continuando con la discusión en el seno de la Comisión se analiza la naturaleza autónoma que debe tener el órgano de control. En este sentido, es importante considerar que en el ordenamiento jurídico chileno la autonomía de los órganos del Estado es un concepto indeterminado, siendo la doctrina y la jurisprudencia las encargadas de darle sentido y contenido, al señalar que dicha autonomía se relaciona con la independencia que el órgano o entidad tiene del Presidente de la República, en efecto, en el ámbito de la Administración del Estado los órganos autónomos son independientes del Presidente de la República, pero esta independencia no es uniforme, lo que significa que la autonomía tiene en el sistema chileno distinta intensidad, es decir, hay órganos que tienen más independencia que otros.

Lo anterior además se configura con otro elemento que se produce en la estructura institucional chilena, que es que existen órganos con autonomía constitucional y órganos con autonomía legal. En efecto, hay órganos autónomos, porque la Constitución los declara como tales, como es el caso de la Contraloría General de la República, el Banco Central o el Ministerio Público y hay otros cuya autonomía es declarada por la ley, como es el caso del Instituto Nacional de Derechos Humanos, el Consejo para la Transparencia o el Consejo del Servicio Electoral. En este sentido, es posible advertir que en la institucionalidad chilena los órganos autónomos según la ley, más recientemente creados, tienen estándares de independencia muy similares a los órganos autónomos constitucionales, lo que pareciera ser una tendencia del legislador en el sentido de darle mayor espacio de deliberación en sus decisiones y sin que su remoción dependa directamente del ejecutivo.

En este mismo sentido, durante el análisis efectuado en la Comisión sobre la independencia de la Autoridad de Control para la protección de datos, se tuvo en consideración que las órganos con autonomía legal en el sistema chileno, tienen por finalidad ser coadyuvantes de la Administración, contando con facultades de fiscalización que garanticen derechos fundamentales. Cuestión que explica, además, la relación que dichos órganos con autonomía legal tienen con los denominados controles no institucionales sobre la Administración, como el que realizan los medios de comunicación o la sociedad civil organizada, por ejemplo, cuando las organizaciones medioambientales, a través de presentaciones ante la Corte Interamericana de DD.HH., promovieron el acceso a la información de los órganos del Estado, siendo la antesala de la dictación de la Ley N° 20.285 sobre Transparencia y Acceso a la Información Pública y la creación del Consejo para la Transparencia[650]. Por consiguiente, sería posible

[650] Un ejemplo en esta materia es el caso Claud Reyes y Otros Vs. Chile, seguido ante la Corte Interamericana de Derechos Humanos, que en lo sustancial trata de lo siguiente: El 8 de julio de 2005, de conformidad con lo dispuesto en los artículos 50 y 61 de la Convención Americana, la Comisión Interamericana de Derechos Humanos sometió ante la Corte una demanda contra el Estado de Chile. Dicha demanda se originó en la denuncia

afirmar que el antecedente o detonante de la generación de entidades autónomas como el Consejo para la Transparencia o el Instituto Nacional de DD.HH. proviene de las demandas sociales, y en ese sentido, al no ocurrir lo mismo con la generación de una autoridad de control en materia de protección de datos personales, se estaría optando por una entidad dependiente del Ministerio de Hacienda sin la autonomía ni facultades suficiente para abordar esa temática[651].

Otro aspecto que se aborda en la tramitación legislativa del proyecto, a propósito de la Agencia de Protección de Datos que se propone por el Ejecutivo, es que su creación no estaría mediada por un mecanismo que sea capaz de resolver los conflictos entre esta y el Consejo para la Transparencia, incentivando la resolución de estos por la vía judicial, confrontando a dos órganos del Estado ante los tribunales de justicia, afectando el desarrollo de la política pública.

Sobre la dependencia de la Agencia del Ministerio de Hacienda, la experiencia comparada muestra que el hacerse cargo de la protección de datos personales requiere de entidades que tengan mayor cercanía y sensibilidad con la temática, teniendo en cuenta el tratamiento de datos de los ciudadanos desde la perspectiva de su condición de consumidores o en la configuración de la protección de datos personales como Derecho Fundamental, por lo que aparecería más adecuada en el contexto de la institucionalidad chilena, la dependencia de la Autoridad de Control que se pretende crear, a ministerios como el de Economía o Justicia y Derechos Humanos. Ya que si bien Hacienda es un ministerio que cuenta con un fuerte prestigio institucional sus competencias para el diseño y formulación de políticas públicas y protección de los derechos fundamentales son ajenas al mandato institucional del Ministerio de Hacienda, el cual se orienta a la dirección de la política financiera, de recaudación de rentas públicas y de contabilidad general, entre otras, pero no a la tutela del derecho a la protección de datos personales.

No. 12.108, recibida en la Secretaría de la Comisión el 17 de diciembre de 1998. La Comisión presentó la demanda con el fin de que la Corte declare que el Estado es responsable por la violación de los derechos consagrados en los artículos 13 (Libertad de Pensamiento y de Expresión) y 25 (Derecho a la Protección Judicial) de la Convención Americana, en relación con las obligaciones establecidas en los artículos 1.1 (Obligación de Respetar los Derechos) y 2 (Deber de Adoptar Disposiciones de Derechos Interno) de la misma, en perjuicio de los señores Marcel Claude Reyes, Sebastián Cox Urrejola y Arturo Longton Guerrero. Los hechos expuestos por la Comisión en la demanda habrían ocurrido entre mayo y agosto de 1998 y se refieren a la supuesta negativa del Estado de brindar a los señores Marcel Claude Reyes, Sebastián Cox Urrejola y Arturo Longton Guerrero toda la información que requerían del Comité de Inversiones Extranjeras, en relación con la empresa forestal Trillium y el Proyecto Río Condor, el cual era un proyecto de deforestación que se llevaría a cabo en la décimo segunda región de Chile y "podía ser perjudicial para el medio ambiente e impedir el desarrollo sostenible de Chile". La Comisión indicó que tal negativa se dio sin que el Estado "argumentará una justificación válida de acuerdo con la legislación chilena", así como a que supuestamente "no otorgó un recurso judicial efectivo para impugnar una violación del derecho al acceso a la información" y "no les aseguró los derechos al acceso a la información y a la protección judicial, ni contó con mecanismos establecidos para garantizar el derecho al acceso a la información pública". Asimismo, la Comisión solicitó a la Corte que, de conformidad con el artículo 63.1 de la Convención, ordene al Estado que adopte determinadas medidas de reparación indicadas en la demanda. Por último, solicitó al Tribunal que ordene al Estado el pago de las costas y gastos generados en la tramitación del caso en la jurisdicción interna y ante los órganos del Sistema Interamericano.

[651] Hay que considerar que la conformación de una Agencia de Protección de Datos Personales responde a una exigencia de inserción internacional de Chile en el marco de los compromisos de la OCDE. Su objetivo mayor es el regular los flujos de intercambio internacional de datos para ser considerado país seguro.

Tanto las Directrices de la OCDE sobre protección de la privacidad y flujos transfronterizos de datos personales, como el nuevo Reglamento General de Protección de Datos de Europa, señalan que la Autoridad de Protección de Datos Personales debe tutelar los derechos y las libertades fundamentales de las personas físicas en lo que respecta al tratamiento y facilitar la libre circulación de datos personales, y que para cumplir su rol deben ser ajenos, en el desempeño de sus funciones y en el ejercicio de sus poderes, a toda influencia externa, ya sea directa o indirecta. Asimismo, en cuanto a su configuración, la autoridad de control debe disponer de los recursos humanos, técnicos y financieros, así como de la infraestructura necesaria para el cumplimiento efectivo de sus funciones y el ejercicio de sus poderes. Además, las decisiones que adopte deben ser objetivas e imparciales contando con los poderes necesarios para establecer las sanciones que correspondan.

Destacable en este punto fue la intervención ante la Comisión del Adjunto de la Agencia Española de Protección de Datos, señor Jesús Rubí, quien expresó que, desde el punto de vista de su configuración, unipersonal o colegiados, no hay un único modelo recomendable de autoridad que articule la protección de datos. Agregó que en el artículo 8° de la Carta de Derechos Fundamentales de la Unión Europea se reconoce el derecho a la protección de datos y se señala que lo tutelará una autoridad independiente, siendo lo fundamental de las distintas autoridades de protección de datos, la forma en que son nombradas; en su mandato; en el formato de garantías de los titulares del órgano; en que sus decisiones solo sean revisables ante la jurisdicción y que se le otorgue un ámbito de control al parlamento directo sobre el funcionamiento de dicha Autoridad.

Señaló que, en el caso de España, el funcionamiento unipersonal ha generado una enorme eficiencia en relación con otros órganos colegiados de la Unión Europea, donde la toma de decisiones es bastante más compleja, porque la composición se articula en torno a la representación de uno u otro sector.

En este mismo sentido, si la entidad de control se configura como una autoridad unipersonal, es indispensable que se establezcan condiciones para su inamovilidad distintas a los ciclos de cambios de gobierno y que las causales de remoción estén previamente establecidas en la legislación y que sean objetivas, evitando o al menos disminuyendo la eventual captura política de quienes están a cargo de la institución.

El proyecto establece un procedimiento distinto de reclamo frente a infracciones al derecho fundamental a la protección de datos personales, expresada, entre otras, en la diferenciación para el ejercicio de los derechos ARCO entre el sector público y el sector privado. Tal diferenciación resulta arbitraria ya que si el tratamiento es por entidades privadas se consagra el derecho a presentar reclamación ante la autoridad de control, pero si la afectación al derecho a la protección de datos deriva del tratamiento efectuado por organismos públicos se establece un procedimiento de tutela judicial. Esta distinción resulta inexplicable y odiosa e implica que si quien deniega el ejercicio de los derechos reconocidos por la ley de protección de datos es un ente privado, puede acudir a la Autoridad de Protección de Datos en búsqueda de amparo, pero si quien vulnera los derechos de las personas es un organismo público, se debe acudir a los tribunales de justicia, lo que significa que el afectado debe tener recursos suficientes para pagar a un abogado especializado y someter el asunto a las ritualidades y costos propios de un juicio, deduciendo un reclamo de ilegalidad ante las Cortes de Apelaciones respectiva.

En definitiva, debe otorgarse a la Autoridad de Control suficientes poderes de investigación, supervisión, resolución, promoción y sanción para dirigirse sobre entidades públicas y privadas

que en el tratamiento de datos afecten el derecho a la autodeterminación informativa de los titulares de los datos.

Otro de los aspectos que se abordaron durante el análisis de la discusión legislativa es el que dice relación con la necesidad de que Chile cuente con un nivel adecuado de protección de datos, especialmente necesario para la transferencia internacional de los mismos y las implicancias económicas que ello tiene. En efecto, el consejero del Instituto Chileno de Derecho y Tecnología, señor Carlos Reusser, en su intervención en la Comisión del Senado señaló que no es efectivo lo sostenido por el Ministerio de Hacienda en sesión pasada, en el sentido de que Chile solo tiene que responder internacionalmente, en materia de protección de datos, frente a los requerimientos de la Organización para la Cooperación y el Desarrollo Económicos (OCDE) o que esta ley debe aprobarse como "un buen comienzo". Añadió que Chile pertenece tanto al sistema de la Organización de las Naciones Unidas y también a la Organización de Estados Americanos, y la primera de ellas ya ha emitido Directrices para la regulación de los archivos de datos personales informatizados en 1990[652] y luego una Resolución A/C.3/68/L.45/Rev.1 sobre el Derecho a la Privacidad en la Era Digital, en 2013[653].

A su vez, la Organización de Estados Americanos ha normado la materia, tanto a través de la AG/RES. 2842 (XLIV-O/14)[654] sobre acceso a la información pública y protección de datos personales como también estableciendo los Principios de la OEA sobre la Privacidad y la Protección de Datos Personales[655].

A mayor abundamiento, un tratado vigente, el Acuerdo por el que se establece una Asociación entre la Comunidad Europea y sus Estados miembros, por una parte, y la República de Chile, por otra, publicado en el Decreto 28 de 2003, del Ministerio de Relaciones Exteriores[656], dice textualmente en el Artículo 202 "Las Partes acuerdan otorgar un elevado nivel de protección al procesamiento de datos personales y de otra índole, compatible con las más altas normas internacionales".

La votación en la Comisión sobre la Autoridad de Control

Avanzada la tramitación en primer trámite constitucional del proyecto de ley, se procede a la votación al interior de la Comisión de Constitución, Legislación, Justicia y Reglamento del Senado de cada uno de los artículos del proyecto. En lo que interesa para el desarrollo de esta investigación se abordará la discusión sobre los artículos referidos a la Autoridad de Control para la protección de datos, preceptos 30 y siguientes del proyecto de ley.

---

[652] Adoptada mediante la Resolución 45/95 de la Asamblea General de 14 de diciembre de 1990, ver en: D.3BIS_ Directrices de Protección de Datos de la ONU.doc (udg.mx) consulta realizada el 29 de enero de 2021.

[653] Ver en: Etpu (oas.org), consulta realizada el 29 de enero de 2021.

[654] Ver en: Declarations & Resolutions - 44 General Assembly - Spanish (oas.org) consulta realizada el 29 de enero de 2021.

[655] Ver en: Microsoft Word - Document2 (oas.org) consulta realizada el 29 de enero de 2021.

[656] Ver en: Decreto-28 01-FEB-2003 MINISTERIO DE RELACIONES EXTERIORES - Ley Chile - Biblioteca del Congreso Nacional (bcn.cl) consulta realizada el 29 de enero de 2021.

En efecto, el artículo 30 del proyecto encabeza el nuevo Título VI, en él se crea la Agencia de Protección de Datos Personales y se definen sus características institucionales. Su texto es el siguiente:

"Artículo 30. Agencia de Protección de Datos Personales. Créase la Agencia de Protección de Datos Personales, organismo público, de carácter técnico, descentralizado, con personalidad jurídica y patrimonio propio, encargado de velar por el cumplimiento de la normativa relativa al tratamiento de los datos personales y su protección, sometido a la supervigilancia del Presidente de la República a través del Ministerio de Hacienda y afecto al Sistema de Alta Dirección Pública establecido en la ley N° 19.882.

El domicilio de la Agencia de Protección de Datos Personales será la ciudad de Santiago."

Al iniciarse el estudio de este precepto, los representantes del Ejecutivo propusieron a la Comisión aprobar el proyecto del Ejecutivo, enmendado en los siguientes términos:

"Artículo 30. Agencia de Protección de Datos Personales. Créase la Agencia de Protección de Datos Personales, organismo público descentralizado, de carácter técnico, con personalidad jurídica y patrimonio propio, *independiente de todo órgano o servicio*[657], sometido a la supervigilancia del Presidente de la República a través del Ministerio de Hacienda, encargado de velar por el cumplimiento de la normativa relativa al tratamiento de los datos personales y su protección.

El domicilio de la Agencia de Protección de Datos Personales será la ciudad de Santiago".

Señalan que los cambios más sustanciales de la propuesta del Ejecutivo dicen relación con haber recogido las opiniones vertidas en las audiencias previas, con la finalidad de reforzar el carácter autónomo de la mencionada institución. Expresan que cuando se habla de autonomía, se refieren a una autonomía de carácter administrativo, y no política, teniendo en cuenta el carácter unitario del Estado chileno. Agregan que el Gobierno está compuesto por el Presidente de la República y sus ministros, y en el ámbito territorial, por los Intendentes y Gobernadores, estando la Administración del Estado constituida por un complejo orgánico de instituciones que se encuentran bajo la dependencia o bajo la tutela del Presidente de la República, y que es en el ámbito de la Administración del Estado donde se radica la Agencia.

Desde el punto de vista normativo, señalan que ella se acerca a un modelo institucional similar al de la Fiscalía Nacional Económica[658]. Esta última es parte de la Administración del Estado,

---

[657] La cursiva es nuestra.

[658] La Fiscalía Nacional Económica (FNE) es la agencia chilena encargada de defender y promover la libre competencia en todos los mercados o sectores productivos de la economía chilena.

La Ley de Defensa de la Competencia (DL 211) establece que la FNE es un servicio público descentralizado, con personalidad jurídica y patrimonio propio, independiente de todo organismo o servicio, que se encuentra sometida a la supervigilancia del Presidente de la República a través del Ministerio de Economía, Fomento y Turismo. Para cumplir con su labor, la FNE investiga todo hecho, acto o convención que impida, restrinja o entorpezca la libre competencia, o que tienda a producir dichos efectos. Entre sus focos de investigación se cuentan las prácticas colusorias, los abusos de posición monopólica y las concentraciones que afecten o puedan afectar el funcionamiento eficiente de los mercados y el bienestar del consumidor. La FNE lleva a cabo también diversas acciones de ***Advocacy***, para difundir los beneficios de la competencia, con el objetivo de crear en el país una "cultura de competencia". Dentro de ellas, se cuentan una serie de iniciativas destinadas a la comunidad y

se relaciona con el Presidente de la República, a través del Ministerio de Economía, y se encuentra bajo la supervigilancia de la máxima autoridad, mas no bajo su potestad jerárquica.

Los representantes del Ejecutivo indican que los criterios para establecer la autonomía de un órgano de la Administración del Estado, son los siguientes: Servicio descentralizado (personalidad jurídica y patrimonio propio)[659]; Dependencia de la autoridad del servicio, sea unipersonal o colegiada, con el Presidente de la República (nombramiento y remoción) y participación de otros Poderes del Estado, Senado o Corte Suprema; Revisión de las actuaciones y decisiones de la autoridad del servicio; y Gestión presupuestaria.

Agregan que se está ante una Agencia cuyo nombramiento depende del Presidente de la República, a través de la Alta Dirección Pública y la remoción de sus miembros está determinada por causales específicas, remoción en la que participa la Corte Suprema. Sobre la autonomía técnica señalan que la Agencia es un órgano que no está sujeto a ninguna otra autoridad. Añaden que el período de duración en el cargo del Director/a se fijó en 5 años, para otorgarle mayor autonomía a la Agencia, desacoplándola del ciclo político.

Sobre esta propuesta, asesores del comité de oposición durante la discusión en la Comisión, previo a la votación, plantearon que el ideal para una institucionalidad que se haga cargo de la protección de datos es que cuente con autonomía y con una estructura de gobierno compuesta por un Director y un Consejo Directivo, cuestión que no aparece recogida en la propuesta del Ejecutivo, en este sentido plantean que la jurisprudencia tanto del propio Consejo para la Transparencia como de los tribunales de justicia, dan cuenta de que la función de proteger los datos de los titulares, puede ser atribuida al señalado Consejo y que en definitiva la relación de la Agencia con el Ministerio de Hacienda aminorará la autonomía de la misma.

Por su parte, el ejecutivo plantea que esa misma jurisprudencia demuestra que el Consejo para la Transparencia ha privilegiado el acceso a la información, por sobre la protección de datos.

Además, sobre la relación de la Agencia de Protección de Datos con el Ministerio de Hacienda se hace presente que España acaba de actualizar su legislación en materia de protección de datos y que el modelo de la Agencia Española consiste en una autoridad administrativa independiente del ámbito estatal, de régimen jurídico del sector público, con personalidad jurídica y plena capacidad pública y privada, que actúa con plena independencia de los poderes públicos en el ejercicio de sus funciones, que se relaciona con el Gobierno a través del Ministerio de Justicia.

A mayor abundamiento, la autoridad que se propone es autónoma en el mecanismo de nombramiento y de remoción y no está sujeta a la jerarquía ni a la decisión arbitraria de la máxima autoridad, siendo sus decisiones inimpugnables, solo sujetas al control jurisdiccional. Respecto al gobierno corporativo, se estimó que una autoridad colegiada no implica mayor

---

colaboración con otros organismos gubernamentales. Ver en: Fiscalía Nacional Económica (fne.gob.cl) consulta realizada el 01 de febrero de 2021.

[659] Sobre esta característica, como ya se ha señalado en este trabajo de investigación, en el sistema chileno no necesariamente un órgano autónomo es descentralizado, por ejemplo la Contraloría General de la República es autónoma según se dispone en el artículo 98 de la Constitución, no obstante es centralizada desde la perspectiva que no tiene personalidad jurídica propia, actúa con la personalidad jurídica del Estado, ni tampoco tiene patrimonio propio, por cuento sus recursos previenen únicamente de la ley anual de presupuestos de la nación, que es de iniciativa exclusiva del Presidente de la República. Ver en: Contraloría General de la República de Chile - www.contraloria.cl

calidad técnica, ni mejores decisiones. Ello dice relación exclusivamente con el marco institucional.

Finalmente, tras revisar exhaustivamente las opciones institucionales disponibles, se optó por el modelo mayoritario en el mundo, a saber, que el acceso a la información y la protección de datos estén bajo órganos distintos.

En una sesión posterior, el Ejecutivo presentó una indicación para sustituir la redacción de este precepto por la siguiente:

"Articulo 30. Agencia de Protección de Datos Personales. Créase la Agencia de Protección de Datos Personales, organismo público autónomo, descentralizado, de carácter técnico, con personalidad jurídica y patrimonio propio, sometido a la supervigilancia del Presidente de la República a través del Ministerio de Hacienda, encargado de velar por el cumplimiento de la normativa relativa al tratamiento de los datos personales y su protección. La Agencia estará afecta al Sistema de Alta Dirección Pública, sin perjuicio de las normas que se establecen en esta ley.

El domicilio de la Agencia de Protección de Datos Personales será la ciudad de Santiago".

Como se puede apreciar de esta nueva redacción del artículo 30, la propuesta del ejecutivo incorpora la expresión "autónomo".

El señor presidente de la Comisión, Senador Felipe Harboe valoró esta redacción pues incorpora la expresión "autónomo", de manera que se consagra la autonomía legal del órgano. Consideró relevante que cuando se discuta las funciones y atribuciones, se analice la institución desde el prisma eminentemente técnico. Constató que se necesitarán expertos que entiendan el equilibrio que debe existir entre el flujo de datos y la protección de los derechos de los titulares de datos.

El asesor del Ministerio de Hacienda agregó que en la redacción original se señalaba que la Agencia estaba afecta al sistema de Alta Dirección Pública. Reseñó que con posterioridad se sugirió eliminarlo, porque se reguló en otro artículo el nombramiento del Director de la Agencia mediante ese procedimiento.

La nueva propuesta del Ejecutivo consiste en reincorporar, al final del inciso primero, la siguiente frase: "La Agencia estará afecta al Sistema de Alta Dirección Pública, sin perjuicio de las normas que se establecen en esta ley." Explicó que el Director de la Agencia será elegido mediante un procedimiento especial en el que participa el Senado, entre otros. Añadió que el segundo nivel jerárquico también sigue afecto al sistema de Alta Dirección Pública.

El Presidente de la Comisión, Senador señor Harboe declaró cerrado el debate y puso en votación el artículo 30. La Comisión, por la unanimidad de sus miembros presente, Senadores señores Araya, De Urresti, Harboe y Larraín, aprobó la indicación del Ejecutivo.

Lo relatado da cuenta que en la primera votación en particular se aprueba en la Comisión de Constitución, Legislación, Justicia y Reglamento del Senado, la creación de una Agencia de Protección de Datos Personales, entidad autónoma sobre la cual el Presidente de la República ejercer la supervigilancia a través del Ministerio de Hacienda.

El criterio anteriormente descrito varió durante su tramitación en el año 2018, donde con el cambio de Gobierno y una nueva configuración en el Senado, este presentó indicaciones formuladas el 03 de julio de 2018, durante la discusión en general del proyecto de ley, en primer trámite constitucional, que regula la protección y el tratamiento de los datos personales

y crea la agencia de protección de datos personales[660]. En específico la indicación consiste en que la función de Autoridad de Control se radicase en el Consejo para la Transparencia, organismo encargado de resguardar el derecho al acceso a la información pública y la transparencia de los órganos de la Administración del Estado.

Si bien ya se abordaron los principales argumentos esgrimidos durante la discusión en la Comisión de Constitución, Legislación, Justicia y Reglamento del Senado, hay uno en particular que fue especialmente reiterado y que dijo relación con temas de índole presupuestario, en el sentido de que representaría un menor costo para el Estado asignar la protección de los datos de carácter personal a una entidad ya existente en vez de crear una nueva entidad de la Administración Pública.

De esta modificación da cuenta el Segundo Informe de la Comisión de Constitución, Legislación, Justicia y Reglamento del Senado, que señala: "La indicación número 185, de Su Excelencia el Presidente de la República, lo reemplaza por el siguiente: Artículo 30. Autoridad de Control. El Consejo para la Transparencia y la Protección de Datos Personales, creado en la ley N° 20.285 sobre Acceso a la Información Pública, será el órgano encargado de velar por el cumplimiento de la normativa relativa al tratamiento de datos personales y su protección, como de todos los derechos consagrados en esta ley".

El Presidente de la Comisión, Senador señor Harboe, la puso en votación, ya que está en línea con lo resuelto por la Comisión en torno a la institucionalidad. La Comisión, por la mayoría de sus miembros, Senadores señores Allamand, Huenchumilla y Pérez, la aprobó. Votaron en contra los Senadores señores De Urresti y Harboe.

Como consecuencia de la decisión anteriormente adoptada, la Comisión decidió, en virtud de lo dispuesto en el inciso final del artículo 121 del Reglamento del Senado, reemplazar en todo el proyecto de ley las menciones a "la Agencia de Protección de Datos Personales" por "el Consejo para la Transparencia y la Protección de Datos Personales".

Independientemente de que la institucionalidad aprobada, que es la que actualmente se encuentra vigente en la tramitación del proyecto de ley, que continua en Primer trámite constitucional en la Comisión de Hacienda del Senado[661], y que por consiguiente, puede incorporársele modificaciones durante las etapas legislativas que vienen, resulta importante para el desarrollo de esta investigación realizar las siguientes consideraciones sobre asignar la regulación de la protección de datos al Consejo para la Transparencia:

1. Como primera consideración cuyas reflexiones ya han sido presentadas anteriormente se puede precisar que el Consejo para la Transparencia desde sus orígenes ha promovido y regulado la mayor divulgación posible de la información sustentada en las directrices de la información pública y la transparencia de las entidades de la Administración del Estado.

[660] Ver en: Senado - Tramitación de proyectos consulta realizada el 01 de febrero de 2021.

[661] El 16 de marzo del año 2021 pasa de la Comisión de Constitución, Legislación, Justicia y Reglamento del Senado a la Comisión de Hacienda del Senado.

2. Dichas directrices son contradictorias y hasta antagónicas con la intimidad y la vida privada, así como con la confidencialidad de la información, que son los ejes sobre los cuales se sustenta la protección de datos de carácter personal.

3. De lo anterior es dable colegir que la institucionalidad para el abordaje de la protección de datos personales requiere altos estándares de independencia y especialización, que se centren exclusivamente en tutelar el derecho fundamental a la protección de datos personales.

4. La complejidad de los contenidos a abordar y los fenómenos jurídicos y técnicos asociados requieren de una entidad reguladora altamente calificada y con experiencia en la promoción y resguardo del derecho a la protección de datos que podrá tutelar incluso otros derechos o afectar el ejercicio de ellos.

5. La independencia de la autoridad de control para la protección de datos es esencial en un mercado de servicios de la información que se incrementa exponencialmente y que en el contexto de la pandemia derivada del COVID19 ha tenido todavía un mayor desarrollo, lo que requiere una independencia que le impida ser capturada por ciclos o presiones políticas.

6. Para asegurar esa independencia, elementos como la designación de la autoridad de control, su exclusividad para el desempeño de sus funciones, su inamovilidad, las causales de remoción y otros aspectos vinculados a su presupuesto y atribuciones, no aparecen evidentes en el actual Consejo para la Transparencia chileno[662].

7. Por todas estas consideraciones y otras, que serán desarrolladas en el apartado de las conclusiones de esta investigación, no parece adecuado radicar la función de promover y regular la protección de datos personales en el actual Consejo para la Transparencia chileno.

A continuación, y considerando el contexto chileno se analizará la importancia de la independencia o autonomía que debe tener una autoridad de control en materia de protección de datos de carácter personal y como se deberán ponderar los factores técnico-políticos en su estructuración y designación.

[662] En efecto, el Consejo para la Transparencia está integrado por cuatro consejeros que no tienen exclusividad en el desempeño de sus funciones, pudiendo incluso asesorar a entidades públicas o privadas en temas relacionados con transparencia y acceso a la información pública. Además, la integración de Consejo se hace bajo variables políticas, en el sentido de que, desde su creación, dos consejeros son proclives al gobierno y los otros dos son de oposición. Finalmente, una vez que cesan en sus funciones pueden desarrollar actividades profesionales en el ámbito profesional privado en asuntos relacionados con las funciones que les correspondió desempeñar como consejeros.

Hacia una Autoridad de Control Independiente para la Protección de Datos Personales

Para el análisis que nos ocupa, esto es la independencia o autonomía de una autoridad de control en materia de protección de datos, se enfocará el análisis en la designación de su máxima autoridad, sea esta unipersonal o colegiada, haciendo una revisión de la experiencia chilena en la materia durante los últimos años, lo que será un insumo más para concluir sobre la conveniencia o no de que sea el Consejo para la Transparencia o una Autoridad nueva la que asuma la regulación de la protección de datos de carácter personal.

Autores como Weber plantean que la independencia de un órgano de la Administración permite asegurar mayor objetividad en el ejercicio de la función pública que se debe desempeñar, de ahí la configuración de la denominada carrera funcionaria que permitiría al funcionario público realizar sus labores haciendo prevalecer criterios técnicos por sobre consideraciones políticas, evitando su captura por los gobiernos de turno que administran la infraestructura estatal[663].

Desde una perspectiva más actual, la independencia[664], además de lo ya revisado en el Capítulo IV de este trabajo, referido a las agencias independientes[665], se refiere a una serie de instrumentos que protegen a la entidad o agencia de la influencia del poder ejecutivo y especialmente del poder gubernamental principalmente en tres ámbitos: a) designación de autoridades, b) capacidad regulatoria o toma de decisiones, y c) presupuesto. En el sistema chileno es posible advertir la configuración de estos tres ámbitos. Sobre la designación de sus autoridades, lo que se busca es involucrar en el nombramiento a los otros poderes públicos morigerando la intervención del ejecutivo, como por ejemplo ocurre con los consejeros del Banco Central que deben ser confirmados por el Senado.

En cuanto a su capacidad de toma de decisiones, este se relaciona con la facultad para adoptar decisiones dentro de su ámbito competencial sin la participación o injerencia vinculante del ejecutivo, caso paradigmático en este sentido son los dictámenes de la Contraloría General de la República, que además van generando la denominada jurisprudencia administrativa.

Con respecto al presupuesto, lo que se busca es que la agencia esté habilitada para allegar sus propios recursos sin que estén condicionados a la ley anual de presupuestos, que es de iniciativa exclusiva del ejecutivo y que puede ser utilizada como un incentivo o un desincentivo para la gestión de la señalada agencia.

Otro aspecto que es importante considerar en el diseño institucional del Estado chileno es que las agencias o entidades autónomas o independientes de naturaleza regulatoria también tienen diversa configuración, a las ya señaladas como el Banco Central o la Contraloría General de la República, que son entidades que tienen mayores niveles de independencia, estructurándose como órganos autónomos constitucionales integrantes de la Administración Pública, se

---

[663] Weber, M. (1964), *"Economía y Sociedad"*, José Medina y Otros (traducción), Fondo de Cultura Económica, México, pp. 1-45. Ver en: https://www.flacso.edu.mx/sites/default/files/extras/weber_conceptos_sociologicos.pdf.

[664] Pardow, D. (2018), "¿Técnicos o políticos?: Radiografía del Sistema de Nombramiento de Directores de Agencias Regulatorias Independientes", *Revista Chilena de Derecho*, Vol. 45 N°3, pp.745-769.

[665] Ahí se analizó que la independencia en la literatura comparada se configuraba fundamentalmente sobre la base de tres elementos: neutralidad política, especialización técnica y eficacia.

agregan también los órganos descentralizados donde el Presidente de la República ejerce sobre ellos la supervigilancia a través del respectivo ministerio y que se organizan bajo la denominación de superintendencias, cuya actividad regulatoria es realizada por una autoridad unipersonal, a estas se agregan otras entidades, organismos que ejercen funciones públicas distintas a la función gubernamental, por ejemplo jurisdiccionales, como ocurre con el Tribunal de Defensa de la Libre Competencia.

Las Agencias Reguladoras Independientes en Chile

Esta denominación, si bien no es explícita en el ordenamiento jurídico chileno, ya que la legislación que regula la materia, esto es, la Ley de Bases Generales de la Administración del Estado, Ley Orgánica Constitucional N° 18.575, solo distingue entre servicios públicos centralizados y descentralizados, y la configuración administrativa dependiendo de la independencia que estos tengan del Presidente de la República, los denomina órganos autónomos constitucionales o legales. La función de regular determinados sectores o ámbitos de interés público hace que estas entidades puedan asumir tres clasificaciones o categorías: a) Superintendencias; b) Autonomías constitucionales; y c) Entidades colegiadas.

a) Las Superintendencias y otras entidades similares

Las Superintendencias son un servicio público descentralizado, dirigido por una autoridad unipersonal, son expresión de la evolución de un Estado prestador de servicios públicos hacia uno que regula a las entidades privadas encargadas de otorgar esas prestaciones públicas, fenómeno que se generaliza con las privatizaciones de las empresas del Estado durante la década de los ochenta[666]. Es decir, las superintendencias regulan un determinado sector que realiza una determinada prestación que se considera relevante en el ámbito de las necesidades públicas a satisfacer por el Estado y que este ha delegado en los privados quedando estos afectos a su regulación.

En el diseño institucional chileno es posible distinguir las siguientes superintendencias; la Superintendencia de Seguridad Social, SUSESO[667]; Superintendencia de Electricidad y

[666] En la experiencia comparada, ejemplos paradigmáticos de ello ocurren en el Reino Unido con Thatcher y en EE. UU. con Reagan, en lo que autores como Moran denominan "*new public management"*, en el caso chileno la principal diferencia con dichos modelos es la discrecionalidad con la que se nombran sus titulares, discrecionalidad que no existe en los casos mencionados. Ver en: Moran, M. (2003), "*The British regulatory state: high modernism and hyper-innovation*", Oxford, Oxford University Press on Demand.

[667] La Superintendencia de Seguridad Social es una institución descentralizada del Estado, con personalidad jurídica y patrimonio propio, que se relaciona con el ejecutivo a través del Ministerio del Trabajo y Previsión Social a cargo de fiscalizar el cumplimiento de la normativa de seguridad social y garantizar el respeto de los derechos las personas, especialmente de los pensionados y sus familias. Ver en: SUSESO: Prensa - Prensa consulta realizada el 02 de febrero de 2021.

Combustibles, SEC[668]; Superintendencia de Educación, SUPEREDUC[669]; Superintendencia de Educación Superior, SESUPERIOR[670]; Superintendencia de Insolvencia y Reemprendimiento, SUPERIR[671]; Superintendencia de Servicios Sanitarios, SISS[672];

[668] La Superintendencia de Electricidad y Combustibles, SEC, nace el 14 de diciembre del año 1904 bajo el mandato del Presidente Germán Riesco, con el nombre de Inspección Técnica de Empresas y Servicios Eléctricos. Desde aquel entonces, y con el correr de los años, la SEC ha ido evolucionando en sus funciones hasta convertirse en la principal agencia pública responsable de supervigilar el mercado de la energía. Ochenta y un años después de su nacimiento, el 22 de mayo de 1985, es publicada en el Diario Oficial La Ley Nº 18.410 que crea la Superintendencia de Electricidad y Combustibles, Institución que se relaciona con el Gobierno por intermedio del Ministerio de la Energía. La responsabilidad de la SEC se ejerce sobre el mercado de la energía. Ver en: Acerca de SEC: Superintendencia de Electricidad y Combustibles consulta realizada el 02 de febrero de 2021.

[669] La Superintendencia de Educación fue creada por la Ley Nº 20.529 publicada el 27 de agosto de 2011, cuya entrada en funciones se inició el 1 de septiembre de 2012. Esta institución se crea como parte del Sistema Nacional de Aseguramiento de la Calidad, compuesto también por el Ministerio de Educación, Agencia de la Calidad y Consejo Nacional de Educación. Su objeto es fiscalizar, de conformidad a la ley, que los sostenedores de establecimientos educacionales reconocidos oficialmente por el Estado se ajusten a las leyes, reglamentos e instrucciones que dicte la Superintendencia, y fiscalizar la legalidad del uso de los recursos de los establecimientos que reciban aporte estatal. Asimismo, su labor es promocionar, informar y educar, en el ámbito de su competencia, a todos los integrantes de las comunidades educativas y ciudadanía en general, sobre la normativa educacional y el resguardo de derechos. También, debe dar a conocer los mecanismos disponibles para resolver consultas, solicitar mediaciones y atender denuncias o reclamos. La Superintendencia es un servicio público, funcionalmente descentralizado y territorialmente desconcentrado, dotado de personalidad jurídica y patrimonio propio, y que se relaciona con el Presidente de la República por intermedio del Ministerio de Educación. Ver en: Conoce la Superintendencia de Educación – Superintendencia de Educación (supereduc.cl) consulta realizada el 02 de febrero de 2021.

[670] La Superintendencia de Educación Superior es un organismo público creado por la ley N° 21.091, sobre Educación Superior, orientada a fiscalizar y supervigilar el cumplimiento de las disposiciones legales y reglamentarias que regulan a las universidades, institutos profesionales y centros de formación técnicas del país, así como fiscalizar porque éstas destinen sus recursos a los fines que les son propios, de acuerdo a la ley y sus estatutos. Esta institución se crea como parte del Sistema Nacional de Aseguramiento de la Calidad de la Educación Superior, compuesto también por el Ministerio de Educación, la Comisión Nacional de Acreditación y el Consejo Nacional de Educación. Este nuevo organismo fiscalizador tiene como propósito contribuir a la mejora de la calidad de la educación impartida en la educación superior colaborando, junto al resto de los órganos pertenecientes al Sistema de Aseguramiento de la Calidad de la Educación Superior, a aumentar la transparencia y la confianza que las personas y la ciudadanía en el sistema, resguardando a su vez la fe pública depositada por la sociedad en las diversas instituciones de educación superior del país. En el ejercicio de su función fiscalizadora y de supervigilancia, la Superintendencia respeta la autonomía de las instituciones de educación superior y la libertad académica que la Constitución y la ley les reconoce, cautelando y promoviendo la diversidad de proyectos educativos. Ver en: Conoce a la Superintendencia de Educación Superior - Superintendencia de Educación Superior (sesuperior.cl) consulta realizada el 02 de febrero de 2021.

[671] La Superintendencia de Insolvencia y Reemprendimiento es un servicio público, descentralizado con personalidad jurídica propia y que se relaciona con el Presidente de la República a través del Ministerio de Economía, Fomento y Turismo, velando por la efectividad y transparencia de los procedimientos concursales y de quiebras, a través de la fiscalización y facilitación de acuerdos en resguardo de sus intervinientes, promoviendo el reemprendimiento mediante la superación de la situación de insolvencia y sobreendeudamiento de personas y empresas. Ver en: Superir | Superintendencia de Insolvencia y Reemprendimiento consulta realizada el 02 de febrero de 2021.

[672] La Superintendencia de Servicios Sanitarios tiene como misión velar porque la población urbana abastecida por las empresas de servicios de agua potable y saneamiento de las zonas urbanas del país reciba dichos servicios con la calidad y continuidad establecido en la normativa, a precio justo y sostenible en el largo plazo; adicionalmente, asegurar a la comunidad, que el agua una vez utilizada será tratada para ser devuelta a la

Superintendencia de Salud, SUPERSALUD[673]; Superintendencia de Medioambiente, SMA[674] y Superintendencia de Pensiones, SPENSIONES[675]; Superintendencia de Casinos de Juegos,

naturaleza de forma compatible con un desarrollo sustentable. Esta responsabilidad será cumplida buscando promover la transparencia en el mercado, el autocontrol por parte de las empresas y desarrollando una actuación eficiente. Ver en: Misión, visión, valores - Superintendencia de Servicios Sanitarios (siss.gob.cl) consulta realizada el 02 de febrero de 2021.

[673] La Superintendencia de Salud, tiene por función; 1. Supervigilar y controlar a las instituciones de salud previsional, en los términos que señale el Capítulo VII del Libro I y el Libro II del DFL 1/2005 y las demás disposiciones legales que sean aplicables, y velar por el cumplimiento de las obligaciones que les imponga la ley en relación a las Garantías Explícitas en Salud, los contratos de salud, las leyes y los reglamentos que las rigen; 2. Supervigilar y controlar al Fondo Nacional de Salud (en adelante FONASA) en todas aquellas materias que digan estricta relación con los derechos que tienen los beneficiarios del Libro II del DFL 1/2005 en las modalidades de atención institucional, libre elección, lo que la Ley establezca como Garantías Explícitas en Salud y al Sistema Ley 20.850 de Protección Financiera para Diagnósticos y Tratamientos de Alto Costo; 3. Fiscalizar a todos los prestadores de salud públicos y privados, sean estos personas naturales o jurídicas, respecto de su acreditación y certificación, así como la mantención del cumplimiento de los estándares establecidos en la acreditación; y 4. Controlar y supervigilar el Sistema de Protección Financiera para Diagnósticos y Tratamientos de Alto Costo. Para estos efectos, podrá regular, fiscalizar y resolver las controversias respecto de prestadores, seguros, fondos e instituciones que participen de todos los sistemas previsionales de salud, incluyendo los de las Fuerzas Armadas, Carabineros de Chile, Policía de Investigaciones y Gendarmería de Chile. Ver en: Definiciones estratégicas - Superintendencia de Salud, Gobierno de Chile (supersalud.gob.cl) consulta realizada el 02 de febrero de 2021.

[674] La Superintendencia del Medio Ambiente (SMA) es un servicio público descentralizado, con personalidad jurídica y patrimonio propio, sometido a la supervigilancia del presidente de la República a través del Ministerio del Medio Ambiente, y cuyos cargos directivos son provistos de acuerdo con el sistema de Alta Dirección Pública. A la SMA le corresponde de forma exclusiva ejecutar, organizar y coordinar el seguimiento y fiscalización de las Resoluciones de Calificación Ambiental, de las medidas de los Planes de Prevención y/o de Descontaminación Ambiental, del contenido de las Normas de Calidad Ambiental y Normas de Emisión, y de los Planes de Manejo, cuando corresponda, y de todos aquellos otros instrumentos de carácter ambiental que establezca la ley. Ver en: ¿Qué es la SMA? | Superintendencia Del Medio Ambiente consulta realizada el 02 de febrero de 2021.

[675] La Superintendencia de Pensiones es el organismo contralor que representa al Estado al interior del sistema de pensiones chileno. Es una entidad autónoma, cuya máxima autoridad es el superintendente o superintendenta. Se relaciona con el gobierno a través del Ministerio del Trabajo y Previsión Social, por intermedio de la Subsecretaría de Previsión Social. La Superintendencia de Pensiones fue creada por la Ley N° 20.255 de marzo del 2008, como sucesora y continuadora legal de la Superintendencia de Administradora de Fondos de Pensiones, creada por el Decreto Ley N° 3.500, de 1980, que inició sus funciones el 1 de mayo de 1981. Se rige por un estatuto orgánico contenido en el Decreto con Fuerza de Ley N° 101 de 1980, del Ministerio del Trabajo y Previsión Social. Ver en: La institución - SP. Superintendencia de Pensiones - Gobierno de Chile (spensiones.cl) consulta realizada el 02 de febrero de 2021.

SCJ[676]. A estas se suman otros organismos descentralizados[677] que si bien no se denominan superintendencias también ejercen funciones regulatorias sobre determinados sectores especialmente en el ámbito económico, es el caso de la Comisión para el Mercado Financiero, CMF[678] (que absorbió a la anterior Superintendencia de Bancos e Instituciones Financieras), la Fiscalía Nacional Económica, FNE[679], el Servicio Nacional del Consumidor, SERNAC[680],

[676] Creada a través de la ley N° 19.995 del 07 de enero de 2005, la Superintendencia de Casinos de Juego (SCJ) es el organismo autónomo con personalidad jurídica y patrimonio propio, el cual se relaciona con el Presidente de la República por intermedio del Ministerio de Hacienda. Constituye un servicio público regido por el Sistema de Alta Dirección Pública y representa al Estado en el ejercicio de las funciones de supervigilancia y fiscalización para la instalación, administración y explotación de los casinos de juego del país. Creada a través de la ley N° 19.995 del 07 de enero de 2005, la Superintendencia de Casinos de Juego (SCJ) es el organismo autónomo con personalidad jurídica y patrimonio propio, el cual se relaciona con el Presidente de la República por intermedio del Ministerio de Hacienda. Constituye un servicio público regido por el Sistema de Alta Dirección Pública y representa al Estado en el ejercicio de las funciones de supervigilancia y fiscalización para la instalación, administración y explotación de los casinos de juego del país. Ver en: Acerca de la SCJ | scj consulta realizada el 02 de febrero de 2021.

[677] Tal vez la única excepción sea la Subsecretaria de Telecomunicaciones que, si bien es una entidad centralizada inserta en el Ministerio de Transportes y Telecomunicaciones, ejerce atribuciones de supervisión y tarifarias sobre el sector de las telecomunicaciones.

[678] La Comisión del Mercado Financiero (CMF) es un servicio público descentralizado, de carácter técnico, dotado de personalidad jurídica y patrimonio propio, que se relaciona con el Presidente de la República a través del Ministerio de Hacienda. La Comisión para el Mercado Financiero (CMF) tiene entre sus objetivos principales velar por el correcto funcionamiento, desarrollo y estabilidad del mercado financiero, facilitando la participación de los agentes de mercado y promoviendo el cuidado de la fe pública; además de velar porque las personas o entidades fiscalizadas, desde su iniciación hasta el término de su liquidación, cumplan con las leyes, reglamentos, estatutos y otras disposiciones que las rijan. Ver en: Qué es la CMF - CMF Portal. Comisión para el Mercado Financiero. Gobierno de Chile. (cmfchile.cl) consulta realizada el 02 de febrero de 2021.

[679] La Fiscalía Nacional Económica es la agencia chilena encargada de defender y promover la libre competencia en todos los mercados o sectores productivos de la economía chilena. La Ley de Defensa de la Competencia (DL 211) establece que la FNE es un servicio público descentralizado, con personalidad jurídica y patrimonio propio, independiente de todo organismo o servicio, que se encuentra sometida a la supervigilancia del Presidente de la República a través del Ministerio de Economía, Fomento y Turismo. Para cumplir con su labor, la FNE investiga todo hecho, acto o convención que impida, restrinja o entorpezca la libre competencia, o que tienda a producir dichos efectos. Entre sus focos de investigación se cuentan las prácticas colusorias, los abusos de posición monopólica y las concentraciones que afecten o puedan afectar el funcionamiento eficiente de los mercados y el bienestar del consumidor. La FNE lleva a cabo también diversas acciones de *Advocacy*, para difundir los beneficios de la competencia, con el objetivo de crear en el país una "cultura de competencia". Dentro de ellas, se cuentan una serie de iniciativas destinadas a la comunidad y colaboración con otros organismos gubernamentales. Ver en: Fiscalía Nacional Económica (fne.gob.cl) consulta realizada el 03 de febrero de 2021.

[680] El Servicio Nacional del Consumidor es la agencia del Estado de Chile, encargada de velar por la protección de los derechos de los consumidores. Su misión es informar, educar y proteger a los consumidores, promoviendo el cumplimiento de la normativa vigente, mediante la vigilancia y fiscalización de los mercados, en un marco técnico de eficacia y eficiencia de la acción institucional, potenciando el equilibrio y transparencia en las relaciones de consumo, a través de un SERNAC moderno y ágil al servicio de las personas.

el Servicio Nacional de Aduanas, SNA[681], el Servicio de Impuestos Internos, SII[682] y la Comisión Nacional de Energía, CNE[683]. Estos servicios o comisiones descentralizadas como se ha dicho también realizan funciones de regulación en el ámbito económico al igual que las superintendencias, sin embargo, se diferencian de aquellas por cuanto se distribuyen competencias para proteger un interés de forma transversal, en cambio las superintendencias tienen un diseño institucional en que sus funciones están compartimentadas, focalizando su ámbito de actuación sobre una determinada industria o sector a regular. Por ejemplo, las superintendencias podrán fiscalizar a las administradoras de pensiones, a las universidades o a las empresas de distribución eléctrica en el ejercicio de las funciones que les son propias, en cambio la FNE podrá fiscalizar a cualquiera de ellas si se han coludido para la fijación de precios o el SII podrá fiscalizar también a cualquier sector regulado si ha evadido impuestos.

Órganos con autonomía constitucional

Otra de las categorizaciones que en el sistema chileno admiten las agencias regulatorias independientes son las denominadas autonomías constitucionales[684], especialmente dos

[681] El Servicio Nacional de Aduanas cumple funciones claves en materia de comercio exterior, especialmente, en la facilitación y agilización de las operaciones de importación y exportación, a través de la simplificación de trámites y procesos aduaneros. Asimismo, debe resguardar los intereses del Estado y de la ciudadanía, fiscalizando dichas operaciones, de manera oportuna y exacta, determinando los derechos e impuestos vinculados a éstas y verificando que no ingresen a nuestro país mercancías que puedan ser consideradas peligrosas. Ver en: Rol, facultades y funciones (aduana.cl) consulta realizada el 03 de febrero de 2021.

[682]Su misión es procurar que cada contribuyente cumpla cabalmente sus obligaciones tributarias, aplicando y fiscalizando los impuestos internos de manera efectiva y eficiente, con estricto apego a la legalidad vigente y buscando la facilitación del cumplimiento, en el marco que establecen los principios de probidad, equidad y transparencia, en un ambiente de trabajo que propicie el desarrollo integral de los funcionarios, para lograr un desempeño de excelencia que aporte al progreso del país. Ver en: SII | Servicio de Impuestos Internosconsulta realizada el 03 de febrero de 2021.

[683] La Comisión Nacional de Energía (CNE) es un organismo público y descentralizado, con patrimonio propio y plena capacidad para adquirir y ejercer derechos y obligaciones, que se relaciona con el Presidente de la República por intermedio del Ministerio de Energía. Su Ley Orgánica Institucional corresponde al Decreto de Ley Nº 2.224, de 1978, modificado por la Ley Núm. 20.402, de 2010 que crea el Ministerio de Energía. La Comisión será un organismo técnico encargado de analizar precios, tarifas y normas técnicas a las que deben ceñirse las empresas de producción, generación, transporte y distribución de energía, con el objeto de disponer de un servicio suficiente, seguro y de calidad, compatible con la operación más económica". Mientras que sus funciones son: 1. Analizar técnicamente la estructura y nivel de los precios y tarifas de bienes y servicios energéticos, en los casos y forma que establece la ley; 2. Fijar las normas técnicas y de calidad indispensables para el funcionamiento y la operación de las instalaciones energéticas, en los casos que señala la ley; 3. Monitorear y proyectar el funcionamiento actual y esperado del sector energético, y proponer al Ministerio de Energía las normas legales y reglamentarias que se requieran, en las materias de su competencia; 4. Asesorar al Gobierno, por intermedio del Ministerio de Energía, en todas aquellas materias vinculadas al sector energético para su mejor desarrollo. Ver en: Quienes Somos - Comisión Nacional de Energía (cne.cl) consulta realizada el 03 de febrero de 2021.

[684] Desde luego, no todos los órganos autónomos constitucionalmente pueden ser considerados agencias regulatorias independientes, como ocurre por ejemplo con el Ministerio Público, encargado de ejercer la acción penal en el sistema chileno o el Servicio Electoral SERVEL, cuyas funciones están radicadas en el control y fiscalización de los procesos electorales.

entidades; el Banco Central (BC) y la Contraloría General de la República (CGR)[685], que tienen su origen en la misión Kemmerer[686], misión que configuró un diseño institucional que buscaba limitar la influencia del Poder Ejecutivo, fomentando un compromiso de largo plazo respecto del volumen de gasto público. Así, la función inicial de la Contraloría era verificar la ejecución presupuestaria y revisar la contabilidad general de la nación, y la del Banco Central era contener los incentivos para financiar la expansión del gasto público mediante la emisión de moneda o circulante[687]. Estos órganos constitucionalmente autónomos gozan de amplios niveles de independencia del ejecutivo, ejerciendo funciones de fiscalización. Así, el Banco Central regula la cantidad de dinero en circulación y el crédito en la economía, de manera que sean suficientes para que las personas, empresas e instituciones hagan sus transacciones. Tratándose de la Contraloría, su función reguladora es variada, por ejemplo, en materia de tarifas de servicios básicos, por cuanto los decretos tarifarios están sujetos al trámite de toma de razón[688], que es de su exclusiva y excluyente competencia.

b) Entidades Colegiadas

En este tercer grupo se encuentran entidades que intervienen en ámbitos propios de la regulación económica, son dirigidos por un cuerpo colegiado y su diseño institucional busca establecer mecanismos de independencia formal respecto del Poder Ejecutivo. Es el caso del Tribunal de Defensa de la Libre Competencia, TDLC[689], el Panel Eléctrico y el Consejo para la Transparencia, (CPLT). Un elemento en común que tienen es que fueron impulsados por la incorporación de Chile a la Organización para la Cooperación y Desarrollo Económico, OCDE, tendientes a mejorar la institucionalidad regulatoria del país dotándola de mayores niveles de independencia. Eso sí, el diseño institucional de estos organismos es diverso, en efecto, mientras el CPLT es un organismo legalmente autónomo que forma parte de la estructura de la Administración del Estado, el TDLC es un órgano jurisdiccional y así también es considerado el Panel de Expertos de la Ley General de Servicios Eléctricos, PELGE[690]. Por

[685] También podría ser incluido en la categoría de agencias reguladoras independientes el Consejo Nacional de Televisión cuya misión es velar por el correcto funcionamiento de los servicios de televisión. Ver en: ¿Qué es el CNTV? | Consejo Nacional de Televisión consulta realizada el 03 de febrero de 2021.

[686] La Misión Kemmerer es el nombre dado a una comisión de expertos que hizo propuestas de reformas fiscales y monetarias a varios gobiernos, principalmente en Latinoamérica, entre 1919 y 1931. Dichas «misiones» fueron lideradas por el economista estadounidense Edwin Walter Kemmerer, que fue contratado por varios gobiernos latinoamericanos con el fin de mantener su estabilidad económica.

[687] Drake, P. (1989), "The money doctor in the Andes: the Kemmerer missions, 1923-1933", Duke, Duke University Press.

[688] La Toma de Razón, es el trámite que realiza la Contraloría General de la República para verificar la juridicidad de los actos de la administración del Estado, en este caso el decreto tarifario, en términos que no contradiga la Constitución y las leyes. Este trámite es preventivo, es decir, se realiza antes que el decreto nazca a la vida del derecho, antes de su entrada en vigor, lo que significa que es anterior a su publicación en el Diario Oficial.

[689] El Tribunal de Defensa de la Libre Competencia es un órgano jurisdiccional especial e independiente, sujeto a la superintendencia directiva, correccional y económica de la Corte Suprema, cuya función será prevenir, corregir y sancionar los atentados a la libre competencia

[690] El Panel de Expertos de la Ley General de Servicios Eléctricos es un órgano colegiado autónomo creado en el año 2004 por la Ley Nº19.940, de competencia estricta y reglada. Su función es pronunciarse, mediante

qué no considerar en esta categorización a otros tribunales especializados, como por ejemplo los tribunales ambientales, la respuesta dice relación con que ambas entidades (TDLC y Panel) tienen potestades normativas para establecer reglas de aplicación general, esto es, más allá de la resolución del caso concreto. De esta manera, su capacidad para desarrollar la regulación económica en materia de competencia y electricidad exige considerar ambas instituciones, ya que materialmente realizan funciones que en Derecho Comparado son realizadas por agencias regulatorias independientes. Por otra, el nombramiento de buena parte de los ministros del TDLC corresponde al Banco Central, mientras que el nombramiento de los ministros del Panel de Expertos corresponde al TDLC[691].

A continuación, se expone un cuadro resumen con las denominadas agencias regulatorias independientes revisadas, en la estructura institucional chilena, considerando los siguientes criterios: denominación institucional, estructura institucional, esto es centralizado, descentralizado o autónomo, que se denominará relación con el ejecutivo; año de creación; órgano de dirección unipersonal o colegiada, que se denominara autoridad y ámbito competencial, que se refiere a si regulan un único sector económico (especifico) o ejercen funciones transversales para tutelar un interés determinado, distinción que se nominará función única o transversal, además se revisará si la designación de su titular es por el Sistema de Alta Dirección Pública (SADP), directamente por el ejecutivo (Ejecutivo) o en el nombramiento de su máxima autoridad intervienen otros órganos del Estado, como por ejemplo el Congreso Nacional lo que se denominara designación (Mixta).[692]

Cuadro N° 7

Denominación	Relación con el ejecutivo	Año de creación	Autoridad	Función	Designación
SUSESO	Descentralizado	1953[693]	Unipersonal	Especifico	SADP[694]
SEC	Descentralizado	1985[695]	Unipersonal	Especifico	SADP

dictámenes de efecto vinculante, sobre aquellas discrepancias y conflictos que, conforme a la ley, se susciten con motivo de la aplicación de la legislación eléctrica y de servicios de gas que las empresas eléctricas, de servicios de gas y otras entidades habilitadas sometan a su conocimiento.

[691] Pardow, D. (2018), "¿Técnicos o políticos?: Radiografía del Sistema de Nombramiento de Directores de Agencias Regulatorias Independientes", *Revista Chilena de Derecho*, Vol. 45 N°3, pp.745-769.

[692] Esta información fue extraída de los sitios web de cada uno de los organismos señalados y de una revisión de las leyes que los crean.

[693] Esta entidad surge como organismo público el 10 de diciembre de 1927, con el nombre de Departamento de Previsión Social**.** A partir de julio de 1945, fue denominada Dirección General de Previsión Social**,** hasta que, en el año 1953, se creó la Superintendencia de Seguridad Social**.**

[694] Ver en: SUSESO: Prensa - Concurso cargo Superintendente/a de Seguridad Social consulta realizada el 04 de febrero de 2021.

[695] La Superintendencia de Electricidad y Combustibles, SEC, nace el 14 de Diciembre del año 1904 bajo el mandato del Presidente Germán Riesco, con el nombre de Inspección Técnica de Empresas y Servicios Eléctricos. Desde aquel entonces, y con el correr de los años, la SEC ha ido evolucionando en sus funciones hasta convertirse en la principal agencia pública responsable de supervigilar el mercado de la energía. Ochenta y un años después de su nacimiento, el 22 de Mayo de 1985, es publicada en el Diario Oficial La Ley Nº 18.410 que crea la

SUPEEREDUC	Descentralizado[696]	2011[697]	Unipersonal	Especifico	SADP
SESUPERIOR	Descentralizado	2018	Unipersonal	Especifico	SADP
SUPERIR	Descentralizado	2014[698]	Unipersonal	Especifico	SADP
SUPERSALUD	Descentralizado	2005[699]	Unipersonal	Especifico	SADP[700]
SMA	Descentralizado[701]	2010[702]	Unipersonal	Especifico	SADP
SPENSIONES	Descentralizado	1981[703]	Unipersonal	Especifico	SADP[704]
SCJ	Descentralizado	2005[705]	Unipersonal	Especifico	SADP[706]

Superintendencia de Electricidad y Combustibles, Institución que se relaciona con el Gobierno por intermedio del Ministerio de la Energía.

[696] La Superintendencia es un servicio público, funcionalmente descentralizado y territorialmente desconcentrado, dotado de personalidad jurídica y patrimonio propio, y que se relaciona con el Presidente de la República por intermedio del Ministerio de Educación.

[697] La Superintendencia de Educación fue creada por la Ley Nº20.529 publicada el 27 de agosto de 2011, cuya entrada en funciones se inició el 1 de septiembre de 2012.

[698] En el año 2014 se publica la Ley Nº 20.720 de Reorganización y Liquidación de Activos de Empresas y Personas, y se crea la nueva Superintendencia de Insolvencia y Reemprendimiento. Asimismo, la Superintendencia comienza a relacionarse con el Ministerio de Economía, Fomento y Turismo.

[699] La Superintendencia de Salud es un organismo público, sucesor legal de la Superintendencia de Isapres, que inicia sus operaciones el 1 de enero de 2005, conforme lo establece la Ley de Autoridad Sanitaria (Ley N° 19.937).

[700] El 27 de diciembre de 2019 el Presidente de la República Sebastián Piñera, nombró al abogado Patricio Fernández Pérez como Superintendente de Salud, luego de la presentación de una nómina de candidatos seleccionados a través del Sistema de Alta Dirección Pública (SADP). Ver en: Historia - Superintendencia de Salud, Gobierno de Chile (supersalud.gob.cl) consulta realizada el 04 de febrero de 2021.

[701] La Superintendencia del Medio Ambiente (SMA) es un servicio público descentralizado, con personalidad jurídica y patrimonio propio, sometido a la supervigilancia del presidente de la República a través del Ministerio del Medio Ambiente, y cuyos cargos directivos son provistos de acuerdo con el sistema de Alta Dirección Pública. Se creó en virtud de la Ley Nº 20.417.

[702] Con la publicación de Ley Nº20.417 en el 2010, se crea la Superintendencia del Medio Ambiente (SMA), como un servicio público descentralizado, con personalidad jurídica y patrimonio propio, sometido a la supervigilancia del presidente de la República a través del Ministerio del Medio Ambiente, y cuyos cargos directivos son provistos de acuerdo con el sistema de Alta Dirección Pública.

[703] La Superintendencia de Pensiones fue creada por la Ley N° 20.255 de marzo del 2008, como sucesora y continuadora legal de la Superintendencia de Administradora de Fondos de Pensiones, creada por el Decreto Ley N° 3.500, de 1980, que inició sus funciones el 1 de mayo de 1981. Se rige por un estatuto orgánico contenido en el Decreto con Fuerza de Ley N° 101 de 1980, del Ministerio del Trabajo y Previsión Social.

[704] Osvaldo Macías Muñoz es nombrado Superintendente de Pensiones, de una nómina de candidatos seleccionados por concurso público realizado a través del Sistema de Alta Dirección Pública (ADP). Ver en: Presidenta de la República nombra a Osvaldo Macías como Superintendente de Pensiones - SP. Superintendencia de Pensiones - Gobierno de Chile (spensiones.cl) consulta realizada el 04 de febrero de 2021.

[705] Creada a través de la ley N° 19.995 del 07 de enero de 2005. Ver en: Acerca de la SCJ | scj, consulta realizada el 04 de febrero de 2021.

[706]Constituye un servicio público regido por el Sistema de Alta Dirección Pública y representa al Estado en el ejercicio de las funciones de supervigilancia y fiscalización para la instalación, administración y explotación de los casinos de juego del país.

CMF	Descentralizado[707]	2017[708]	Colegiado[709]	Transversal	Mixta[710]
FNE	Descentralizado[711]	1979	Unipersonal	Transversal	SADP[712]
SERNAC	Descentralizado[713]	1990	Unipersonal	Transversal	SADP[714]

[707]La Comisión del Mercado Financiero (CMF) es un servicio público descentralizado, de carácter técnico, dotado de personalidad jurídica y patrimonio propio, que se relaciona con el Presidente de la República a través del Ministerio de Hacienda.

[708] El 23 de febrero de 2017 se publicó en el Diario Oficial la Ley N°21.000, que crea la nueva Comisión para el Mercado Financiero (CMF), organismo que reemplazó a la SVS. La Comisión para el Mercado Financiero comenzó sus funciones el 16 de enero de 2018.

[709] La dirección superior de la Comisión estará a cargo del Consejo de la CMF, al que le corresponderá ejercer las atribuciones y cumplir las funciones que ésta y otras leyes le encomienden.

[710] El Consejo de la Comisión para el Mercado Financiero (en adelante también el "Consejo") estará integrado por cinco miembros, denominados comisionados, los que se nombrarán y estarán sujetos a las reglas siguientes:1. Un comisionado designado por el Presidente de la República, de reconocido prestigio profesional o académico en materias relacionadas con el sistema financiero, que tendrá el carácter de presidente de la Comisión. El presidente de la Comisión deberá ser nombrado a más tardar dentro de los noventa días siguientes al inicio del período presidencial y durará en su cargo hasta el término del período de quien lo hubiere designado, salvo que concurra alguna de las causales de cesación de funciones establecidas en la presente ley. El Presidente de la Comisión tendrá la calidad de jefe de servicio y gozará de la autoridad, atribuciones y deberes inherentes a esa calidad, en especial los señalados en el artículo 21 y en las demás disposiciones legales pertinentes. 2. Cuatro comisionados designados por el Presidente de la República, de entre personas de reconocido prestigio profesional o académico en materias relacionadas con el sistema financiero, mediante decreto supremo expedido a través del Ministerio de Hacienda, previa ratificación del Senado por los cuatro séptimos de sus miembros en ejercicio, en sesión especialmente convocada al efecto. Los comisionados designados de conformidad con lo dispuesto en este numeral durarán seis años en sus cargos, pudiendo ser reelegidos sólo por un nuevo período consecutivo. Se renovarán en pares, cada tres años, según corresponda. El Presidente de la República deberá proponer al Senado los candidatos que correspondan antes de la expiración del plazo de duración de los comisionados salientes. En caso de que no se efectuaren sus nombramientos antes del vencimiento de dicho plazo, los comisionados salientes podrán permanecer en el desempeño de sus funciones hasta el nombramiento de sus reemplazantes por un plazo máximo de tres meses adicionales. Vencido dicho plazo, y no habiéndose pronunciado el Senado en los términos señalados precedentemente, se nombrará a los candidatos propuestos por el Presidente de la República, sin más trámite. En el nombramiento de los comisionados a que se refieren los números 1 y 2 del presente artículo se deberá velar de manera permanente por la conformación de un Consejo diverso y que equilibre la experiencia y conocimiento técnico que posean sus miembros sobre los mercados específicos que se encuentran sometidos a la fiscalización de la Comisión. El Consejo elegirá de entre sus miembros a un vicepresidente, quien subrogará al presidente en caso de que este último se ausente o esté temporalmente imposibilitado de ejercer sus funciones.

[711] Es un servicio público descentralizado, con personalidad jurídica y patrimonio propio, independiente de todo organismo o servicio, que se encuentra sometida a la supervigilancia del Presidente de la República a través del Ministerio de Economía, Fomento y Turismo.

[712] La Fiscalía Nacional Económica tendrá su sede en Santiago. Estará a cargo de un funcionario denominado Fiscal Nacional Económico, que será nombrado por el Presidente de la República mediante el proceso de selección de altos directivos públicos bajo el Sistema de Alta Dirección Pública. Durará cuatro años en su cargo, pudiendo renovarse su nombramiento por una sola vez.

[713] El Servicio Nacional del Consumidor será un servicio público descentralizado, con personalidad jurídica y patrimonio propio, sujeto a la supervigilancia del Presidente de la República a través del Ministerio de Economía, Fomento y Turismo.

[714] El Director Nacional será el jefe superior del Servicio y tendrá su representación judicial y extrajudicial. Será nombrado por el Presidente de la República a partir de una terna propuesta por el Consejo de Alta Dirección

CNE	Descentralizado[715]	1978	Unipersonal	Transversal	SADP[716]
SNA	Autónomo	1946	Unipersonal	Transversal	SADP[717]
SII	Descentralizado	1902	Unipersonal	Transversal	SADP[718]
BC	Autónomo	1925	Colegiada	Transversal	Mixta[719]
CGR	Autónomo	1927	Unipersonal	Transversal	Mixta[720]
TDLC	Autónomo	2003[721]	Colegiada	Transversal	Mixta[722]
PELGE	Autónomo	2004	Colegiada	Transversal	Mixta[723]

Pública con el voto favorable de cuatro quintos de sus miembros. Durará cuatro años en su cargo y podrá renovarse su nombramiento por una sola vez.

[715] La Comisión Nacional de Energía es un organismo público y descentralizado, con patrimonio propio y plena capacidad para adquirir y ejercer derechos y obligaciones, que se relaciona con el Presidente de la República por intermedio del Ministerio de Energía. Su Ley Orgánica Institucional corresponde al Decreto de Ley Nº 2.224, de 1978, modificado por la Ley Núm. 20.402, de 2010 que crea el Ministerio de Energía.

[716] Su autoridad máxima es el Secretario Ejecutivo que es designado por el Presidente de la República a través del Sistema de Alta Dirección Pública del Servicio Civil.

[717] El Director Nacional de Aduanas es el Jefe Superior del Servicio, y será nombrado por el Presidente de la República, siendo de su exclusiva confianza, previo concurso a través del Sistema de Alta Dirección Pública.

[718] Un funcionario con el título de "Director", es el Jefe Superior del Servicio; será nombrado por el Presidente de la República, siendo de su exclusiva confianza, y será seleccionado, nombrado y remunerado conforme a las normas establecidas en el Título VI, de la Ley N° 19.882, que Regula Nueva Política de Personal a los Funcionarios Públicos, del Sistema de Alta Dirección Pública.

[719] El Consejo estará constituido por cinco consejeros, designados por el Presidente de la República, mediante decreto supremo expedido a través del Ministerio de Hacienda, previo acuerdo del Senado. Los miembros del Consejo durarán diez años en sus cargos, pudiendo ser designados para nuevos períodos, y se renovarán por parcialidades, a razón de uno cada dos años. El Presidente del Consejo, que lo será también del Banco, será designado por el Presidente de la República de entre los miembros del Consejo y durará cinco años en este cargo o el tiempo menor que le reste como consejero, pudiendo ser designado para nuevos períodos.

[720] El Contralor General la República deberá tener a lo menos diez años de título de abogado, haber cumplido cuarenta años de edad y poseer las demás calidades necesarias para ser ciudadano con derecho a sufragio. Será designado por el Presidente de la República con acuerdo del Senado adoptado por los tres quintos de sus miembros en ejercicio, por un período de ocho años y no podrá ser designado para el período siguiente. Con todo, al cumplir 75 años de edad cesará en el cargo.

[721] Fue creado por la Ley N º 19.911, publicada en el D.O. el 14.11.2003, y se instaló el 13 de mayo de 2004.

[722] El Tribunal de Defensa de la Libre Competencia estará integrado por las personas que se indican a continuación: a) Un abogado, que lo presidirá, designado por el Presidente de la República de una nómina de cinco postulantes confeccionada por la Corte Suprema mediante concurso público de antecedentes. Sólo podrán participar en el concurso quienes tengan una destacada actividad profesional o académica especializada en materias de libre. competencia o en Derecho Comercial o Económico, y acrediten a lo menos 10 años de ejercicio profesional. b) Cuatro profesionales universitarios expertos en materias de libre competencia, dos de los cuales deberán ser abogados y dos licenciados o con post grados en ciencias económicas. Dos integrantes, uno de cada área profesional, serán designados por el Consejo del Banco Central previo concurso público de antecedentes. Los otros dos integrantes, también uno de cada área profesional, serán designados por el Presidente de la República, a partir de dos nóminas de tres postulantes, una para cada designación, confeccionadas por el Consejo del Banco Central, también mediante concurso público de antecedentes.

[723] El Panel de Expertos estará integrado por siete profesionales, cinco de los cuales deberán ser ingenieros o licenciados en ciencias económicas, nacionales o extranjeros, y dos abogados, de amplia trayectoria profesional o académica y que acrediten, en materias técnicas, económicas o jurídicas del sector energético, dominio y

CPLT	Autónomo	2009	Colegiada	Transversal	Mixta[724]
SUBTEL	Centralizado	1977	Unipersonal	Única	Ejecutivo
CNTV	Autónomo	1970	Colegiada	Única	Mixta[725]

Fuente: Elaboración propia.

Como se advierte, de las 22 agencias reguladoras independientes analizadas, todas se configuran como entidades autónomas o descentralizadas, salvo la Subsecretaria de Telecomunicaciones, lo que representa una anomalía en el sistema por cuanto es una entidad inserta en el Ministerio de Transportes y Telecomunicaciones, que por consiguiente tiene una dependencia directa del Presidente de la República (el subsecretario que la dirige es designado por este), careciendo de personalidad jurídica y patrimonio propios, que tiene por función regular las tarifas de empresas públicas y privadas en el ámbito de las telecomunicaciones.

Otro aspecto a considerar, es que si bien la Contraloría General de la República es un órgano autónomo, según se dispone en el artículo 98 de la Constitución y también en su Ley Orgánica N° 10336[726], es centralizada, por cuanto no tiene personalidad jurídica propia, actúa con la personalidad jurídica del Estado de Chile y no tiene patrimonio propio, ya que sus recursos son definidos exclusivamente por la ley anual de presupuestos de la nación, así entonces como señala Cordero Quinzacara "… la identificación entre descentralización y autonomía se rompe a partir de los términos de la propia Constitución, pues considera con carácter de autónomo a entidades que no son descentralizadas, como ocurre con la Contraloría General de la República…" y luego agrega "Que tradicionalmente el concepto de autonomía ha estado unida al concepto de descentralización, sin embargo, no necesariamente se identifican, pues existen órganos autónomos que no son descentralizados, como ocurre con la Contraloría General de la República…".[727]

experiencia laboral mínima de tres años. Los integrantes del Panel serán designados por el Tribunal de Defensa de la Libre Competencia, mediante un concurso público de antecedentes fundado en condiciones objetivas, transparentes y no discriminatorias, debiendo velar por que la experiencia mínima de sus integrantes sea representativa de las diversas materias vinculadas al sector energético y respecto de las cuales el Panel es competente para pronunciarse. La convocatoria al concurso público será publicada en un diario de circulación nacional y en un diario de cada región, con cargo al presupuesto del Panel de Expertos. La resolución que los designa será dictada por el Ministerio de Energía.

[724] La dirección y administración superiores del Consejo corresponderán a un Consejo Directivo integrado por cuatro consejeros designados por el Presidente de la República, previo acuerdo del Senado, adoptado por los dos tercios de sus miembros en ejercicio. El Presidente hará la proposición en un solo acto y el Senado deberá pronunciarse respecto de la propuesta como una unidad.

[725] El Consejo se compone de once consejeros**.** Uno de estos, su Presidente, es de libre designación del Presidente de la República y permanece en el cargo hasta 30 días después del cese en el cargo del Primer Mandatario que lo nombró. Los otros diez Consejeros son designados por el Presidente de la República con acuerdo del Senado. Por mandato legal, el Jefe del Estado debe hacer la proposición cuidando que el Consejo quede integrado en forma pluralista. De la misma manera, la ley exige al Presidente del Consejo una idoneidad que garantice el debido pluralismo en el funcionamiento.

[726] Ver en: 1cf9c1df-066b-2057-389e-2c8da9db875b (contraloria.cl) consulta realizada el 05 de febrero de 2021.

[727] Cordero Quinzacara, E. (2012), "La Administración del Estado en Chile y el concepto de Autonomía", en "*La Contraloría General de la República, 85 años de Vida Institucional (1927-2012)"*, pp. 15-33.

De la revisión realizada en este trabajo de investigación, también es posible colegir que cerca del 50% (10) de estas agencias han sido creadas durante los últimos 20 años, mientras que las otras 12 se crearon antes de los últimos dos lustros.

Además, en el diseño institucional la mayoría de estas agencias tienen como superior jerárquico una autoridad unipersonal (17), diseño que se ha mantenido con la creación de las entidades más recientes como las Superintendencias de Educación y de Educación Superior o de Casinos de Juego, siendo tal vez una de las excepciones más recientes las del CPLT, cuya máxima autoridad es un Consejo integrado por 4 miembros o la CMF cuya instancia directiva está conformada por 5 comisionados.

En este mismo sentido, también es importante precisar que las instituciones que cuentan con gobiernos colegiados realizan un mayor número de nombramientos. Ahora bien, la duración en el cargo de los directivos es también diferente. Los directivos duran cerca de 6 años en su cargo cuando se trata de instituciones con gobierno colegiado. Este promedio se reduce a la mitad para instituciones con gobierno unipersonal, donde los directivos duran cerca de 3 años[728].

En el caso del CPLT, es importante considerar que las funciones de esta entidad, establecidas en la ley 20.285 que lo crea, están relacionadas con la transparencia y promoción del acceso a la información de los órganos de la administración pública, siendo un ámbito competencial transversal aplicable sobre cualquier órgano o servicio público. De igual forma, para el desarrollo de esta investigación es importante reiterar que su habilitación, para hacer cumplir las disposiciones de la ley 19.628 en materia de protección de datos personales, es residual y no abarca a las entidades privadas.

Sobre su ámbito competencial, las agencias que se constituyen como superintendencias desarrollan una función específica dirigiendo su accionar sobre una determinada industria o sector económico a regular. En cambio, las entidades que se configuran como servicios, comisiones, consejos o bajo otra denominación, desarrollan su ámbito competencial de manera transversal tutelando un interés genérico cualquiera sea el sector o industria en el que éste se pueda ver amenazado o conculcado, estableciendo estándares regulatorios para cualquier entidad que desarrolle ese interés que se está llamado a proteger.

Finalmente, respecto del sistema de nombramiento de la autoridad de la respectiva agencia, se puede observar una marcada tendencia a ser designadas a través del Sistema de Alta Dirección Pública (14), en una proporción inferior a través de un sistema mixto donde la designación es del ejecutivo pero se requiere la aprobación o intervención de otro poder del Estado como el Senado o la Corte Suprema (7) y en solo un caso se observa la designación exclusiva y excluyente del Presidente de la República. Sobre este punto eso si es importante puntualizar que, en prácticamente todos los casos, la designación o nombramiento propiamente tal es realizado por el Ejecutivo, salvo por una minoría de ministros del TDLC, cuya selección y designación se realiza directamente por el Banco Central. Además, en el caso de la designación bajo la modalidad mixta hay que considerar que los consejeros del Banco Central, del CPLT o la designación del Contralor General de la República en donde interviene también el Senado,

[728]Pardow, D. (2018), "¿Técnicos o políticos?: Radiografía del Sistema de Nombramiento de Directores de Agencias Regulatorias Independientes", *Revista Chilena de Derecho*, Vol. 45 N°3, pp.745-769.

requieren quórums diversos, así, para confirmar un nombramiento para consejero del Banco Central basta la mayoría simple de los senadores, para el CPLT se exigen dos tercios de los senadores en ejercicio y para la designación del Contralor tres quintos de los senadores en ejercicio.

También hay que tener en cuenta que en el proceso de confirmación ante el Senado, la ronda de preguntas de los senadores al candidato se realiza en el hemiciclo o comisión respectiva, antes de proceder a la votación en la Sala. Por otra parte, los procesos de selección realizados por la Corte Suprema suelen incorporar una instancia donde los candidatos realizan una presentación abierta al público. Sin embargo, esa instancia de audiencias, oposiciones y entrevistas públicas no están mayoritariamente incorporadas dentro del procedimiento administrativo chileno para el nombramiento de los titulares de las agencias reguladoras y, son más bien excepcionales.

Para precisar lo señalado precedentemente, es necesario tener en cuenta las siguientes consideraciones; en primer lugar, el SADP en la institucionalidad chilena es relativamente reciente pues surge con la Ley N° 19.882 promulgada en junio del año 2003, la cual creó el Sistema de Alta Dirección Pública (SADP) y la Dirección Nacional del Servicio Civil (DNSC)[729].

A través de este sistema los directivos de las agencias reguladoras participan en un concurso con sucesivas etapas que configuran una terna o quina en la que uno de sus integrantes es designado directamente por el Presidente de la República. La ley N° 20.955[730] introdujo una serie de mejoras al SADP, las que pueden resumirse en las siguientes:

a) Amplía la cobertura del sistema a 124 servicios públicos con 154 nuevos cargos.

b) Elimina la figura de los "Transitorio y Provisionales" y se reemplaza por los subrogantes legales como regla general.

c) Limita concursar cargos vacantes en los últimos 8 meses de gobierno, y si se convocan tales concursos se requerirá la autorización del Consejo de Alta Dirección Pública (CADP) para convocar a los procesos de selección durante ese periodo.

d) La ley establece al Presidente de la República un plazo máximo de 90 días para tomar la decisión de nombramiento o declaración de desierto en cargos de primer nivel jerárquico.

e) Facilita la instalación de los nuevos gobiernos a través de la designación presidencial directa de hasta 12 cargos de Alta Dirección Pública de primer nivel jerárquico, en los tres primeros meses de Gobierno,

[729] El Sistema de Alta Dirección Pública (SADP) tiene como objetivo dotar a las instituciones de gobierno a través de concursos públicos y transparentes de directivos con probada capacidad de gestión y liderazgo para ejecutar de forma eficaz y eficiente las políticas públicas definidas por la autoridad.

[730] Ver en: Ley-20955 20-OCT-2016 MINISTERIO DE HACIENDA - Ley Chile - Biblioteca del Congreso Nacional (bcn.cl) consulta realizada el 08 de febrero de 2021.

f) Permite a los funcionarios públicos nombrados en cargos de Alta Dirección Pública mantener su cargo de planta por 9 años[731].

g) Para mejorar la calidad de los candidatos crea un banco de candidatos y un modelo de gestión de candidatos que evitará declaraciones de concursos desiertos y ayudará a no perder talento directivo detectado y probado.

h) Simplifica el modelo que relaciona el grado de cumplimiento del Convenio de Desempeño y su efecto en las remuneraciones de los cargos de Alta Dirección Pública.

A lo ya señalado, también se debe agregar que los directivos de agencias reguladoras independientes pueden ser destituidos antes de que termine el periodo para el cual fueron designados, eso sí afectos a la respectiva indemnización. En este mismo sentido, también hay que considera que los ciclos presidenciales, es decir, cuando una administración asume el gobierno también previo concurso incide en la designación de los directivos de las agencias regulatorias. En este sentido, el estudio realizado por Pardow[732] señala "La primera tendencia que conviene destacar dice relación con el ciclo electoral que parecieran seguir los nombramientos en nuestras agencias regulatorias. La menor cantidad de nombramientos anuales típicamente ocurre en los últimos años de un período presidencial, mientras que la mayor cantidad típicamente ocurre durante el año de instalación. De hecho, durante los cinco periodos presidenciales[733], la cantidad de nombramientos en el año inicial es significativamente mayor a la cantidad de nombramientos en el año final[734]. Lo mismo se observa si comparamos el volumen de nombramientos de los gobiernos entrantes y salientes: el último año del gobierno saliente supone muchos menos nombramientos que el primer año del gobierno entrante".

Precisamente la independencia de las agencias reguladoras viene determinada por mandatos que no coincidan con los mandatos políticos correspondientes a la Presidencia de la República o a los parlamentarios.

[731] Las plantas de personal en los servicios públicos están definidas en la Ley N° 18.834 que contiene el denominado Estatuto Administrativo que es la norma que regula la función pública en el sistema chileno, el artículo 2° letra b) señala: "b) Planta de personal: Es el conjunto de cargos permanentes asignados por la ley a cada institución, que se conformará de acuerdo a lo establecido en el artículo 5º". Y luego el artículo 5° dispone: "Para los efectos de la carrera funcionaria, cada institución sólo podrá tener las siguientes plantas de personal: de Directivos, de Profesionales, de Técnicos, de Administrativos y de Auxiliares".

[732] Pardow, D. (2018), "¿Técnicos o políticos?: Radiografía del Sistema de Nombramiento de Directores de Agencias Regulatorias Independientes", *Revista Chilena de Derecho*, Vol. 45 N°3, pp.745-769.

[733] Se refiere a los periodos de Aylwin (1990-1994), Frei (1994-2000), Lagos (2000-2006), Bachelet (2006-2010) y Piñera (2010-2014).

[734] En promedio, la cantidad de nombramientos en el último año presidencial son un 72% menos que en el primero. La menor diferencia en este ámbito se observa en el período de Frei, donde alcanza un 57%, la mayor en el primer período de Bachelet, donde alcanza un 87%.

El nuevo artículo 15 Bis de Ley N° 19.496 sobre Protección de los Derechos del Consumidor: la competencia del SERNAC

Una cuestión a estudiar a la hora de configurar una agencia reguladora o una autoridad de control en materia de protección de datos se refiere a su competencia y a la no deseable concurrencia de otros sujetos en la misma materia. Se trata de dotar a un órgano concreto de facultades y poderes suficientes para ejercer su competencia. Al establecer la competencia sobre protección de datos personales no es admisible una dispersión normativa que atribuya la protección de datos personales a varios sujetos, si no existe una razón objetiva. Es cierto que en algunos países como en España se atribuyen competencias a autoridades de control de la protección de datos de Andalucía, Cataluña y el País Vasco, pero el reparto de competencias es claro, se trata de sujetos que se limitan a vigilar el cumplimiento en los organismos públicos de cada una de esas autonomías.

Otra cuestión diferente es cuando no es una razón territorial la que permita la diferenciación, sino que es la materia: en este caso concreto, el consumo y, por tanto las bases de datos personales dedicadas al comercio. Si así se hace, se corre el riesgo de encontrarnos con una diversidad de criterios que impediría aunar razonamientos para promover y fiscalizar la protección de datos personales. De allí entonces la preocupación que genera el proyecto de ley impulsado por el ejecutivo, que reforma la Ley N° 19.496 sobre Protección de los Derechos del Consumidor y que se encuentra en Tercer trámite constitucional en la Cámara de Diputados. Dicha propuesta legislativa dispone lo siguiente:

> *"Artículo 15 bis. Las normas relativas al tratamiento de cualquier tipo de datos personales de los consumidores, incluyendo especialmente los de carácter comercial, contenidas en la ley N° 19.628, sobre protección de la vida privada, en especial en el Titulo III "De la utilización de datos personales relativos a obligaciones de carácter económico, financiero, bancario o comercial", y demás normas legales relacionadas, se considerarán normas especiales de protección de los derechos del consumidor, especialmente para los efectos de lo dispuesto en los artículos 2 bis, 58 y 58 bis de la presente ley.*
>
> *Los proveedores que realicen el tratamiento de cualquiera de los datos mencionados en el inciso anterior deberán dar estricto cumplimiento a las normativas que allí se señalan. Para estos efectos, deberán implementar las medidas necesarias para garantizar la seguridad y la reserva en el tratamiento de datos, con especial resguardo respecto de los fines para los cuales fueron autorizados por su titular.*
>
> *En el supuesto de que los proveedores reporten una violación de seguridad de sus bases de datos o de aquellas de las que se sirvan y que contengan información de sus clientes o usuarios, será mandatorio la entrega de información a los consumidores de lo ocurrido, dentro de 24 horas contadas desde el referido reporte.*
>
> *Esta comunicación se deberá efectuar de forma digital e incluirá las medidas de seguridad adoptadas en momentos previos y posteriores a la ocurrencia del hecho. En caso de no prosperar esta vía de contacto, esta misma información se pondrá en conocimiento del consumidor a través de medios físicos, telefónicos u otros idóneos que garanticen celeridad, dentro de un plazo de 72 horas contado desde el reporte señalado en el inciso anterior.*

Las consultas y reclamos suscitados con ocasión de este tipo de incidentes se canalizarán a través del servicio de atención a los clientes que disponga cada proveedor.

Sin perjuicio de lo consagrado en los incisos anteriores, el responsable tendrá la obligación de informar, a petición del consumidor, la fuente de legitimidad del tratamiento de sus datos y de respetar, en todo caso, la finalidad para la cual fueron recolectados o almacenados".

En primer lugar, para realizar el análisis de esta disposición, hay que considerar que esta legislación en ciernes le otorgaría competencias en materia de protección de datos de los consumidores al SERNAC, cuando paralelamente, como se ha analizado, se está tramitando ante el Senado el proyecto de ley que modifica la Ley 19.628 sobre Protección a la Vida Privada, que crea toda una institucionalidad para regular la autodeterminación informativa. Pudiendo generar una indebida interacción entre cuerpos legales si se incluye una norma en la Ley de Protección al Consumidor que corresponde propiamente a la Ley de Datos Personales, produciendo no solo un conflicto normativo, sino contradicción entre entidades, ya que la protección de datos tendrá una agencia especializada y el SERNAC también estará habilitado para regular dicha materia. Una concurrencia de dos sujetos que nada aporta y que podría generar muchos más problemas que alguna ventaja.

El vigente artículo 15 bis sí que "*establece las competencias legales de otro órgano*" frase que permitiría concentrar las competencias de protección de datos en la nueva institucionalidad para regular la autodeterminación informativa. Al desaparecer dicha norma el SERNAC sería la autoridad competente para regular la protección de datos personales en las relaciones de consumo.

En segundo lugar, según lo indicado en este proyecto de nuevo artículo, las normas de la Ley 19.628 "*se considerarán normas especiales de protección de los derechos del consumidor, especialmente para los efectos de lo dispuesto en los artículos 2 bis, 58 y 58 bis de la presente ley*".

Según lo preceptuado, el artículo 2 bis se hace cargo de regular la aplicación de la Ley de Protección al Consumidor a leyes especiales bajo tres supuestos, contenidos en tres literales: a), b) y c). En la letra a) se refiere a los casos en que la Ley de Protección al Consumidor (LPC) se aplica a aquellos asuntos no previstos en la ley especial. Así, deberá aplicarse la Ley del Consumidor a las relaciones de consumo desarrolladas en el marco de las actividades de tratamiento de datos, en todo aquello que no esté regulado por la Ley de Protección de Datos, pero sí en la LPC. De acuerdo con la letra b), el procedimiento para la defensa de intereses colectivos o difusos de consumidores debiese aplicarse de manera preferente a cualquier otra acción de clase, aun cuando haya legislación especial que contemple este tipo de procedimiento. La letra c), por último, dispone que la LPC se aplicará siempre en aquellos casos en que la legislación especial no contemple procedimientos indemnizatorios a los cuales puedan recurrir los consumidores.

El artículo 58 define las potestades, atribuciones y funciones que corresponden al SERNAC. Con ello, el nuevo artículo 15 bis lo que hace es fijar en dicha entidad la competencia para fiscalizar y velar por el cumplimiento de la Ley de Protección de Datos cuando las actividades de tratamiento de datos se han desarrollado en el contexto de una relación de consumo.

El artículo 58 bis, al que hace mención el nuevo artículo 15 bis indica, en su inciso segundo, que los organismos fiscalizadores sectoriales que tengan facultades sancionatorias deberán

remitir al SERNAC copia de las resoluciones en que impongan sanciones. Con ello, la futura Agencia de Protección de Datos se encontraría en la obligación de remitir al SERNAC copia de aquellas resoluciones en que impongan sanciones a proveedores.

En tercer lugar, el nuevo artículo 15 bis que se quiere aprobar, en forma adicional, establece que los proveedores deberán "*implementar las medidas necesarias para garantizar la seguridad y reserva en el tratamiento de datos, con especial resguardo respecto de los fines para los cuales fueron autorizados por su titular*". De esta forma, sin señalarlo expresamente, se establece la obligación de llevar a cabo una evaluación de riesgos con tal de determinar las medidas de seguridad necesarias, toda vez que será esta la única vía para acreditar la debida diligencia de cara a una brecha de seguridad. Luego, el artículo agrega que *ante brechas de seguridad que expongan datos de clientes o usuarios deberá informarse a los mismos dentro de las 24 horas de ocurrido el hecho por canales digitales y, en caso de no lograr el contacto por este medio, deberá hacerlo dentro de las 72 horas contadas desde el hecho a través de medios físicos, telefónicos u otros idóneos que garanticen celeridad*. Acción que puede ser sumamente gravosa cuando se refiere a un número considerable de consumidores afectados.

En cuarto lugar, de lo anterior se concluye que, en conjunto con la futura Agencia de Protección de Datos, cuando se trate de actividades de tratamiento de datos en el marco de un acto de consumo, el SERNAC desempeñará funciones de fiscalización, además, cualquier resolución que dicha agencia dicte sobre la materia deberá ser remitida a este servicio.

En quinto lugar, si bien se ha indicado que la aplicación de la Ley Nº 19.628 sobre protección a la vida privada es de carácter supletorio, con este nuevo artículo 15 bis se invertiría tal concepto, pasando a concebirse esta ley, al menos en sede de consumo, como una ley especial.

Por último, si ya resulta desafiante la adaptación del tratamiento de datos a los nuevos estándares internacionales de cara a la reforma a la Ley Nº 19.628, hay que tener en especial consideración que el proyecto de ley que establece medidas para incentivar la protección de los derechos de los consumidores no contempla una norma de vacancia legal sobre la materia, como lo hace el proyecto de reforma a la Ley N°19.628 sobre protección de la vida privada, de manera que las disposiciones de este nuevo artículo 15 bis serán aplicables desde el momento de su publicación en el Diario Oficial.

En todo caso, y aun defendiendo una autoridad de protección de datos dotada de independencia, con competencias claras y propias de esa autoridad y que ejerce sus funciones sin injerencias de los poderes públicos, ni de otros órganos autónomos -; debe establecerse en el diseño de la citada autoridad, una cooperación con otras entidades encargadas de otras competencias. Esta es la vía de la española Ley 19/2013 que en su disposición adicional primera señala la cooperación entre la Agencia Española de Protección de Datos. Colaboración que se refuerza con la presencia de un representante de la Agencia Española de Protección de Datos en la Comisión de Transparencia y Buen Gobierno (artículo 36 de la ley 19/2013). Esta idea de colaboración deberá orientar el diseño de la protección de datos en Chile.

Diseño Organizacional y Régimen de Responsabilidad de una Autoridad de Protección de Datos para Chile

Después de revisar la forma y características de las agencias regulatorias en el sistema chileno, se propondrá una estructura orgánica para una Autoridad de Control en materia de protección de datos, con la premisa de configurar una entidad que únicamente regule y promueva la protección de datos y; cuyo titular sea una autoridad unipersonal, ya que como se revisó en líneas precedentes, es el modelo que mejor se aviene a la tradición y cultura de funcionamiento de la Administración pública chilena y. tal vez lo más importante, es la estructura que ha demostrado mejores resultados en la configuración de órganos de control por las razones que precedentemente se expusieron.

Para la configuración de esta propuesta se toma como referencia la estructura de la Agencia Vasca de Protección de Datos[735] así como la legislación latinoamericana más reciente en materia de protección de datos revisada en el capítulo III de esta investigación doctoral, en especial aquella que cuenta con una instancia colegiada y consultiva que asesora y orienta a la autoridad de control como es el caso de México con la Ley General de Protección de Datos Personales en posesión de sujetos obligados de enero del año 2017 que consagra la existencia de un Consejo Consultivo en Protección de Datos. O de manera más reciente la legislación brasilera que en el artículo 58-A de la Ley General de Protección de Datos, de agosto del año 2018, crea el Consejo Nacional de Protección de Datos. O la Ley N° 81 sobre protección de datos de Panamá, del 26 de marzo del año 2019, que en su artículo 35 consagra el Consejo de Protección de Datos como instancia asesora de la Autoridad de Control.

La estructura que se propone es la de una autoridad unipersonal denominada Dirección de la Agencia Nacional de Protección de Datos, cuyo titular sea designado por el Presidente de la República previa ratificación del Senado.

Esta Agencia Nacional de Protección de Datos contará además con un organismo colegiado de carácter consultivo que colaborará con su gestión y asesorará especialmente en relación con la promoción y difusión del contenido y alcance del derecho a la protección de datos y contribuya a crear conciencia y a la generación de una cultura de la privacidad. Este organismo se denominara Consejo Consultivo para la Protección de Datos y estará integrado por representantes de otros poderes del Estado, autoridades independientes con competencias limítrofes, así como miembros de la sociedad civil y de la academia vinculados y conocedores de la protección de datos.

Como unidades o divisiones dependientes de la dirección de la agencia se distinguirá entre: la unidad o división de Asesoría Jurídica, la unidad o división de Registro y Auditoria de Protección de Datos, y una unidad o división de Administración y Servicios.

A la división de Asesoría Jurídica le corresponderá el ejercicio de las funciones de sanción, asesoramiento jurídico sobre consultas que se planteen, redacción de normas de uso, reglamentos y el impulso y la instrucción de los procedimientos derivados de las reclamaciones que formulen las personas para la tutela de sus derechos de acceso, rectificación, supresión,

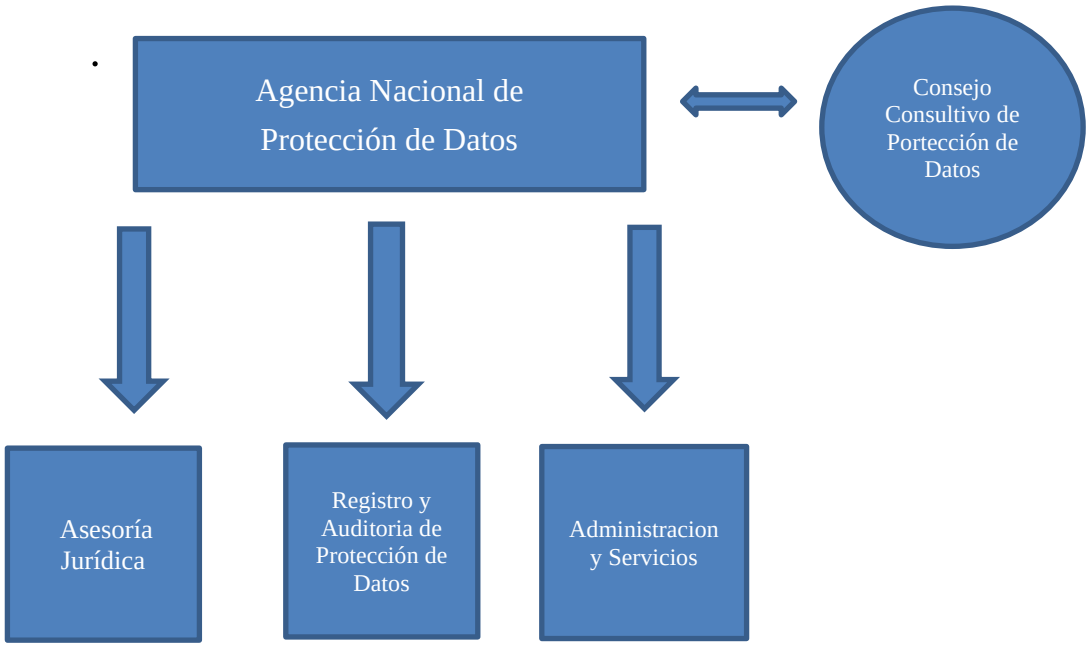
[735] Ver en: https://www.avpd.euskadi.eus/informacion/informacion-institucional-y-organizacional-composicion-y-personal/s04-5216/es/, consulta realizada el 8 de febrero de 2021.

limitación del tratamiento y oposición, así como la instrucción de los procedimientos sancionadores seguidos contra las entidades públicas y privadas y sus encargados del tratamiento, por la vulneración de la normativa de protección de datos personales. También le corresponderá la elaboración de informes, la respuesta a consultas y el asesoramiento jurídico interno de la Agencia Nacional de Protección de Datos.

A la división de Registro y Auditoria de protección de datos le corresponderá hacerse cargo del ejercicio de las funciones de inspección, un registro que dé cuenta de las entidades que cumplen la normativa de protección de datos así como aquellas que la incumplan y que por consiguiente son sancionadas para poner este registro a disposición del público. Por otra parte, tendrá encomendada la realización de estudios relacionados con las nuevas tecnologías y uso del *big data.*

La división de Administración y Servicios será la unidad responsable de las funciones de gestión de recursos humanos y materiales, de gestión económico-administrativa, de las funciones relacionadas con información general, formación y documentación y de funciones de apoyo y ejecución o instrumentales la Agencia.

Organigrama propuesto:



Régimen de Responsabilidad

Como se señalara en el capítulo anterior, la Agencia Nacional de Protección de Datos una vez inserta en la estructura de la Administración Pública chilena, debería en cuanto el ejercicio de sus funciones estar afecta a tres tipos de controles que determinaran eventualmente distintos tipos de responsabilidad.

Ya se señaló que se propone un régimen de rendición de cuentas que considere tres perspectivas:

a) La económica: que fiscalice su patrimonio, para los efectos de que se ejecute adecuadamente su presupuesto y que sus funcionarios o personal dependiente que tenga a su cargo o administre recursos fiscales rinda cuenta de su ejercicio. Para ello será indispensable la evaluación que sobre la ejecución presupuestaria realice la Dirección de Presupuestos DIPRES[736] dependiente del Ministerio de Hacienda. Igualmente respecto de los funcionarios de la Agencia que administran o tiene a su cargo bienes o recursos fiscales será competente para su control la Contraloría General de la República conformándose como Tribunal de Cuentas;

b) La política, para que anualmente reporte sobre su gestión ante el Congreso Nacional a través de una cuenta pública que este contenida en un informe de gestión que incluya los procedimientos administrativos sustanciados para tutelar la protección de datos y el resultado y estadísticas de los mismos; y finalmente

c) c) La Jurídica, este control será ejercido por los tribunales de justicia. Además el personal adscrito a la Agencia, serán responsables por sus actos ante los tribunales y la propia administración.

Una Institucionalidad para la Protección de Datos en el Marco de una nueva Constitución

Evolución política chilena hacia una nueva Constitución

En el contexto del denominado estallido social de octubre del año 2019, Chile avanzó hacia lo que algunos meses antes de la señalada fecha parecía impensado: definir a través de un acuerdo político amplio un itinerario que significase la elaboración de una nueva Carta Política. En efecto, el 15 de noviembre de ese año diversas fuerzas políticas del país firmaron el "Acuerdo por la Paz Social y la Nueva Constitución"[737], la que determinó que en abril del 2020 se realizaría un plebiscito nacional para responder dos preguntas fundamentales: ¿Quiere usted una nueva Constitución? y ¿Qué tipo de órgano debiera redactar la nueva Constitución? una Convención Mixta Constitucional o una Convención Constitucional. La Convención Mixta Constitucional estaría integrada en partes iguales por miembros electos para el efecto, y parlamentarios y parlamentarias en ejercicio. La Convención Constitucional estaría conformada por integrantes electos íntegramente para este efecto. El órgano constituyente que

[736] La Dirección de Presupuestos (Dipres) es el organismo técnico encargado de velar por la asignación y uso eficiente de los recursos públicos, mediante la aplicación de sistemas e instrumentos de gestión financiera, programación y control de gestión, en el marco de la política fiscal.

[737] Ver en: Acuerdo Por la Paz Social y la Nueva Constitución - Avance del proceso constituyente - Proceso constituyente | BCN - Biblioteca del Congreso Nacional de Chile consulta realizada el 14 de febrero de 2021.

elija la ciudadanía tendrá por única función: redactar el nuevo texto constitucional en un plazo de 9 meses, ampliables por una única vez por 3 meses más, plazo que se contará desde el momento en que la Convención se constituya.

Además, el acuerdo dispuso en el punto 10, que: "Los partidos que suscriben el presente acuerdo designarán una Comisión Técnica, que se abocará a la determinación de todos los aspectos indispensables para materializar lo antes señalado. La designación de los miembros de esta Comisión será paritaria entre la oposición y el oficialismo". Dicha comisión, también denominada Mesa Técnica[738] fue la encargada de elaborar y proponer una reforma al Capítulo XV de la Constitución Política de Chile[739], que finalmente se tradujo en la Ley N° 21.200 de Reforma Constitucional publicada el 24 de diciembre de 2019 y promulgada por el Presidente de la República el 23 de diciembre del mismo año, cuyo origen se encuentra en 7 proyectos de ley refundidos, destinados a implementar las propuestas de la Mesa Técnica que posibilitan un procedimiento encaminado a un nuevo texto de Carta Fundamental. Esta Comisión recogió las propuestas de reforma constitucional generadas en el trabajo de la Mesa Técnica[740].

Esta ley convocaba a plebiscito nacional para el día 26 de abril del 2020, sin embargo, esta fecha debió modificarse producto de la pandemia derivada del COVID-19[741], quedando fijada para el día 25 de octubre del año 2020[742], fecha en que se realizó el plebiscito constitucional, cuyos resultados fueron abrumadores para la opción "apruebo": la elaboración de una nueva Constitución y para que esta fuera redactada por una Convención Constitucional integrada por 155 miembros o Convencionales Constituyentes elegidos por votación popular[743]. La elección de los Convencionales Constituyentes se llevó a cabo el 11 de abril de 2021.

Las cifras oficiales del Servicio Electoral de Chile (SERVEL) arrojaron el domingo 25 de octubre del año 2020, históricas cifras de participación de votantes en el Plebiscito Constitucional, que dirimió finalmente la aprobación de la redacción de una Nueva Constitución. De acuerdo con el último balance de SERVEL, votaron más de 7 millones 569 mil personas (7.569.082 de sufragios), lo que representa un 50,95% del padrón total de 14 millones 855 mil (14.855.719); es decir, la elección con mayor votación desde la instauración del voto voluntario en el año 2012. Con el 100% de las mesas escrutadas, la opción "Apruebo" se impuso con el 78,28% de los votos (5.892.832 de votos), mientras la alternativa "Rechazo" alcanzó el 21,72% de las preferencias, con 1.635.164 de sufragios. Por otra parte, ante la

[738] Ver en: Mesa Técnica Constituyente - Avance del proceso constituyente - Proceso constituyente | BCN - Biblioteca del Congreso Nacional de Chile consulta realizada el 14 de febrero de 2021.

[739] Ver en: Propuesta de Mesa Técnica - Avance del proceso constituyente - Proceso constituyente | BCN - Biblioteca del Congreso Nacional de Chile consulta realizada el 14 de febrero de 2021.

[740] Ver en: Publicación de la Ley N° 21.200: Autoriza plebiscito para Nueva Constitución - Avance del proceso constituyente - Proceso constituyente | BCN - Biblioteca del Congreso Nacional de Chile consulta realizada el 14 de febrero de 2021.

[741] Ver en: Plebiscito para el 25 de octubre y elecciones municipales el 11 de abril de 2021 - Senado - República de Chile consulta realizada el 14 de febrero de 2021.

[742] Esta nueva fecha modifico todo el itinerario constitucional y electoral, dejando para el día 11 de abril del año 2021 la elección de los Convencionales Constituyentes.

[743] Ver en: Plebiscito histórico logra la mayor participación electoral en la era del voto voluntario - Avance del proceso constituyente - Proceso constituyente | BCN - Biblioteca del Congreso Nacional de Chile consulta realizada el 14 de febrero de 2021.

pregunta "¿Qué tipo de órgano debiera redactar la Nueva Constitución?" el 79% de los votantes (5.653.542 de votos) optó por una Convención Constituyente, mientras que la Convención Mixta Constitucional alcanzó el 21% (1.502.726 de sufragios).

Afrontando un nuevo derecho fundamental a la protección de datos personales

Así las cosas, Chile tendrá una nueva Constitución que será redactada por primera vez en su historia republicana por ciudadanos electos por votación popular, de carácter paritario y con escaños reservados para los Pueblos Originarios. Este histórico momento desde luego abre una oportunidad para la reconfiguración de los derechos fundamentales y por cierto para potenciar el derecho fundamental a la protección de datos personales. En este sentido, y según se ha desarrollado a lo largo de todo este trabajo de investigación, resulta ineludible proponer una institucionalidad para la protección de datos que también dé cuenta de este cambio constitucional.

Como ya se ha señalado y demostrado en el presente trabajo, si bien Chile fue pionero en Latinoamérica en dictar una ley sobre protección de datos con la entrada en vigor de la Ley N° 19.628 sobre protección a la vida privada[744], resulta evidente que esta ley ha quedado desactualizada, por la irrupción de las redes sociales y el desarrollo de las Tecnologías de la Información y Comunicación (TIC). Esto ha permitido que tanto entidades públicas como privadas almacenen una infinidad de datos de las personas que son tratados sin que existan mecanismos de tutela o garantía adecuados para sus titulares. A ello se añade que a diferencia de la mayoría de los países de la región, recién en el año 2018 la protección de datos personales se reconoce como derecho fundamental. Este reconocimiento significó dotar al titular de los datos personales de la acción de protección, pero que hasta la fecha no ha sido ejercida, no habiéndose presentado recurso de protección alguno invocando la afectación de este, fundamentalmente porque el recurso de protección solo procede frente a una actuación arbitraria o ilegal que perturbe, amenace o transgreda un derecho fundamental, y, en el caso de la protección de datos, puede que la vulneración se produzca por el tratamiento de la información que se está haciendo sin el consentimiento de su titular o porque el titular de los datos quiere acceder a su propia información, en definitiva, la acción de protección no alcanza a cubrir todas las hipótesis de afectación del derecho a la protección de datos.

Otras de las razones que han impedido la adecuada tutela de esta garantía constitucional (la de la protección de datos personales) es el desconocimiento que se observa desde los tribunales de justicia respecto del abordaje de este derecho fundamental que en muchos casos es confundido con el respeto y protección a la vida privada, el honor personal y familiar e incluso el derecho a la imagen que es un derecho constitucionalmente implícito, este desconocimiento o al menos la deficiente delimitación normativa que se observa de estos derechos se expresa en que desde la inclusión del derecho fundamental de la protección de datos de carácter personal a la Constitución chilena en el año 2018, hasta al menos el año 2020, no se había

[744] Como se puede apreciar, el título de la ley limita la protección de datos a la vida privada y no reconoce, el legislador de la época, seguramente de manera involuntaria, la autonomía e independencia de este derecho.

presentado ningún recurso de protección para tutelar este derecho, ni tampoco se registra jurisprudencia alguna que lo reconozca de manera indubitable.[745]

Como se ha señalado el texto que se plasmó en el N° 4 del artículo 19 de la Constitución Chilena: "El respeto y protección a la vida privada y a la honra de la persona y su familia y asimismo, la protección de sus datos personales. El tratamiento y protección de estos datos se efectuará en la forma y condiciones que determine la ley"[746]. A continuación de la expresión "*asimismo*", le reconoce a la protección de datos, tal como lo había hecho la doctrina y los ordenamientos jurídicos comparados, independencia y autonomía, dotándolo de un contenido y alcance propios. Reconociéndolo no solo en su dimensión negativa, para que no se utilicen esos datos sin el consentimiento de su titular, sino que, en su dimensión positiva, esto es el derecho a disponer de los mismos, consagrando así la libertad de los datos o la autodeterminación informativa[747].

El Habeas data en Chile y Latinoamérica

Como ya se ha señalado, en Chile el ejercicio de la acción de hábeas data está regulado en el artículo 16 de la Ley 19.628, pudiendo revestir dos modalidades: una preventiva, cuando tenga por objeto permitir al titular de los datos personales ser informado sobre la existencia de bancos o registros de datos que contengan información que le concierne y si así fuese, acceder a los mismos; y una correctiva, cuando a través de él se exige que determinados datos personales sean corregidos, bloqueados, cancelados, pues el tratamiento que se hace de ellos es indebido, en el sentido que vulnera o conculca sus derechos. A pesar de esta regulación legal, como se sabe, en la práctica, el ejercicio de esta acción es casi inexistente, tanto por déficit procedimental en su configuración como por que las sanciones a las que están expuestos los responsables de los ficheros o bases de datos son irrisorias, inhibiendo a los titulares de los datos de su ejercicio.

[745] De este desconocimiento e inadecuada delimitación normativa da cuenta Contreras, Bordachard y Ortiz editores (2022) en *"Privacidad y protección de datos personales. Jurisprudencia seleccionada y comentada"* DER ediciones, Santiago de Chile,

[746] El 16 de junio de 2018 se publicó en el Diario Oficial la ley 21.096, que consagra la protección de datos personales como garantía constitucional, en el numeral 4° del artículo 19 de la Constitución chilena.

[747] La Convención Conctitucional chilena esta proponiendo en el nuevo texto constitucional una reconfiguración del derecho a la protección de datos de carácter personal, del siguiente tenor: "Derecho a la autodeterminación informativa. Toda persona tiene derecho a la protección de los datos personales. Este derecho comprende la facultad de acceder a los datos recogidos que le conciernen, ser informada y oponerse al tratamiento de sus datos y a obtener su rectificación, cancelación y portabilidad, sin perjuicio de otros que establezca la ley. El tratamiento de datos personales sólo podrá efectuarse en los casos que establezca la ley, sujetándose a los principios de licitud, lealtad, calidad, transparencia, seguridad, limitación de la finalidad y minimización de datos"

Autores como Villegas Carrasquilla plantean un tercer modelo en materia de protección de datos, para diferenciarlo del modelo europeo[748] y estadounidense[749]: el latinoamericano. Este se sustentaría en el derecho fundamental de *habeas data,* que además de ser un derecho fundamental, es una acción de protección de la que gozan los titulares de los datos, frente al tratamiento indebido o ilegal de los mismos, alojados en archivos de entidades tanto públicas como privadas[750].

Latinoamérica se diferencia del modelo europeo, fundamentalmente porque no existe una norma, tratado o instrumento multilateral (aparte de las regulaciones de *soft law*, como la de la Red Iberoamericana de Protección de Datos) de carácter general que resguarde la protección de datos de carácter personal.

En efecto, el reconocer el derecho a la protección de datos en las Cartas Políticas de la región, aun cuando no sea explícitamente, así como la incorporación del habeas data, es un proceso que se observa desde la década de los ochenta y que se extiende incluso hasta el presente siglo veintiuno, eso sí, la forma, contenido y alcance de este reconocimiento constitucional no es uniforme.

A diferencia de los países europeos, que fijaron como mecanismo de regulación y promoción para la protección de datos personales el establecimiento de una autoridad de control en la materia, en Latinoamérica se ha utilizado este instrumento jurisdiccional, el habeas data, y que está presente en las constituciones de Argentina (art. 43), Bolivia (art. 130), Brasil (art. 5° N°71), Ecuador (art. 92), Honduras (art. 182 N°2), Paraguay (art. 135), Perú (art. 200 N°3) o Republica Dominicana (art.70) por mencionar algunas[751].

De lo expuesto, es posible colegir que el derecho a la protección de datos personales puede ser reconfigurado, tomando en cuenta el momento constitucional por el que atraviesa Chile, no solo para mejorar su conceptualización a través de la expresión de autodeterminación informativa, si no para consagrar con rango constitucional su contenido, reconociendo los derechos de acceso, rectificación, cancelación[752] y oposición (ARCO), así como los principios

[748] El sistema europeo tiene un alcance más general y uniforme, que ha sido reforzado por el Reglamento General de Protección de Datos Personales RGPD 2016/679 de la UE, donde se tutela y reconoce el derecho a la protección de datos por parte del Estado, el cual interviene activamente en su promoción y protección.

[749] El enfoque norteamericano se sustenta fundamentalmente en la noción de libertad como contrapartida a la intervención estatal en la vida de las personas, promoviendo principalmente la autorregulación, por lo que la afectación de la protección de datos personales es resuelta por los tribunales de justicia.

[750] Villegas Carrasquilla, L. (2012), "Protección de datos personales en América Latina: retención y tratamiento de datos personales en el mundo de Internet", en *"Hacia una Internet Libre de Censura, Propuesta de América Latina"*, Facultad de Derecho, Centro de Estudios en Libertad de Expresión y Acceso a la Información, compilador Eduardo Bertoni, Buenos Aires, p.130.

[751] Detalles del panorama constitucional latinoamericano en materia de protección de datos y habeas data se desarrolla en el Capítulo III de esta investigación doctoral.

[752] Sobre el derecho de cancelación supresión, en la experiencia comparada, fundamentalmente europea, se reconfigura un nuevo derecho derivado de la Autodeterminación informativa, el derecho al olvido, el cual no tiene reconocimiento expreso en el ordenamiento jurídico chileno, pero que es posible de conceptualizar como el derecho de las personas físicas a hacer que se borre la información sobre ellas después de un periodo de tiempo. Si bien la ley 19.628 no lo señala expresamente, en su artículo 21 dispone una figura que podría ser asimilable al señalar: "Los organismos públicos que sometan a tratamiento datos personales relativos a condenas por delitos,

de licitud y consentimiento, sino que además regulando en la Carta Política el habeas data, como una acción para su efectiva tutela que sea coadyuvante para la protección de este, conjuntamente con una Autoridad de Control.

Consideraciones finales

En definitiva, las agencias regulatorias independientes en Chile tienen un alto grado de especialización, encontrándose restringido su ámbito de intervención sobre un mercado, industria o interés específico. Su diseño institucional responde al de un servicio público funcionalmente descentralizado, en la mayoría de los casos con una autoridad unipersonal que las dirige, designada por el ejecutivo, observándose una tendencia en los últimos años a que el proceso de selección de dicha autoridad se realice a través del Sistema de Alta Dirección Pública.

Por consiguiente, para la estructuración de una autoridad de control para la protección de datos en Chile, resulta indispensable concebirla como una agencia regulatoria independiente, con altos estándares de especialización y con un diseño de gobierno, sea unipersonal o colegiado, que no se vea afectado por los cambios de gobierno, que goce de inamovilidad y que las causales de remoción estén taxativamente establecidas en la respectiva legislación. En este sentido, y considerando la revisión realizada, pareciera que lo más aconsejable sobre su ámbito competencial es que este sea acotado a salvaguardar un interés específico o regular un sector económico o industria más bien determinado, por lo que no parece lo más conveniente que al Consejo para la Transparencia (CPLT) se le asigne la función de tutelar la protección de datos de carácter personal, por cuanto desde su creación sus funciones han estado focalizadas en regular y promover la transparencia y el acceso a la información público.

De igual forma, las nuevas competencias que se le pretenden asignar al Servicio Nacional del Consumidor (SERNAC) en materia de protección de datos no solo generarán eventuales conflictos normativos, sino que producirá una dispersión institucional donde existirán varias agencias habilitadas para regular la protección de datos, lo que supondrá también diversos criterios a la hora de aplicar la normativa y lo que es más complejo aún, disparidad de visiones para aplicar las sanciones que correspondan.

Si no se atribuyen todas las competencias de protección de datos personales a la futura Autoridad de Control de protección de datos personales, se creará un problema competencial. Cuando la protección de datos afecte al consumo la competencia corresponderá al SERNAC, pero es que en muchos casos el tratamiento de datos personales no solo tiene que ver el consumo, también con el cobro de deudas, estudios de mercado, socios o seguidores… asuntos y objetivos que incluyen el consumo, pero también exceden el consumo. A esta consideración debemos añadir que muchos de los problemas tienen su origen en el ámbito del consumo, por lo que el vaciamiento de competencias de la Autoridad de Control la hará ineficaz[753].

infracciones administrativas o faltas disciplinarias, no podrán comunicarlos una vez prescrita la acción penal o administrativa, o cumplida o prescrita la sanción o la pena".

[753] El 24 de diciembre del año 2021 entro en vigencia la ley N° 21.398 que entrega atribuciones en materia de protección de datos para los consumidores.

Finalmente, el *momentum* constitucional por el que atraviesa Chile configura una oportunidad inigualable para repensar la protección de datos y formular una institucionalidad que desde la nueva Constitución asegure su adecuada promoción y tutela. Para lo cual se propone:

1. Consagrar de manera expresa en el catálogo de derechos fundamentales la autodeterminación informativa y además hacer referencia a su contenido estableciendo los denominados derechos ARCO.

2. Disponer que a través de la respectiva ley se estructurará una entidad o autoridad de control encargada no solo de proteger y fiscalizar tanto a instituciones públicas como privadas en el cumplimiento efectivo del respeto a la protección de datos personales como derecho fundamental sino además se encargue de su promoción y del desarrollo de acciones preventivas para su adecuado resguardo.

3. Incorporar en la nueva Carta Política el habeas data como una acción que permita tutelar el derecho a la Autodeterminación informativa.

Por último a la hora de la configurar la Autoridad de Control de protección de datos personales existe la doble disyuntiva de configurarla como un modelo mixto –que agrupe competencias de protección de datos, además de las propias del acceso a la información pública- o único – solo la protección de datos y, en segundo lugar, si se establece un órgano de dirección colegiada o unipersonal. La decisión debe de ponderar no solo los modelos que ofrece el derecho comparado, el análisis de los pros y los contras, también la propia idiosincrasia del pueblo chileno, del funcionamiento de sus instituciones, todo ello en interés de Chile.

Argumentos a favor de un modelo mixto

Como se ha señalado, lo que esta investigación doctoral propone es la configuración de una institucionalidad, de una autoridad de control que se configure bajo lo que se ha denominado modelo único. No obstante, existen argumentos para instalar en Chile un órgano que regule la protección de datos conjuntamente con el derecho de acceso a la información pública, es decir se estructure una institucionalidad mixta. Estos argumentos pueden sistematizarse de la siguiente manera:

a) La creación de una nueva Agencia puede resultar ineficiente porque generará más gasto público, se producirán curvas más largas de instalación y aprendizaje institucional, y podría generar conflictos con el CPLT institución que actualmente tiene facultades en la materia respecto de los datos personales tratados en el sector.

b) Adicionar a la institucionalidad de acceso a información pública (CPLT) la protección de datos personales, puede realizarse con menos gasto público, mayor eficiencia, más eficacia y cumpliendo con los estándares de independencia y autonomía que se exigen internacionalmente.

c) Es posible aventurar que de asumir el CPLT la función de autoridad de control en

materia de protección de datos personales, mediante el ejercicio de las facultades de promoción y protección de los derechos y, de sanción en casos de incumplimientos, el estándar de amparo del derecho a la protección de datos personales debiera experimentar un alza considerable.

d) En el mismo sentido, un modelo mixto permitiría resolver de manera expedita los conflictos entre derechos, lo que facilitaría, a su vez, generar lineamientos generales o específicos que la institucionalidad debiera recoger e implementar en su quehacer cotidiano. Si consideramos que casi un cuarto de los casos que actualmente conoce el CPLT se refieren a datos personales, este es un aspecto de relevancia.

Argumentos a favor de un modelo único.

El presente trabajo propone y promueve estructurar un modelo institucional que regule la protección de datos de manera exclusiva, asumiendo competencias de protección que pudiera tener otros órganos, como es el caso del SERNAC, configurándose bajo el denominado modelo único, a continuación se exponen los principales argumentos para esta formulación:

a) El acceso a la información pública y la protección de datos personales son derechos distintos, el primero promueve la transparencia y el fortalecimiento del Estado de Derecho a través de un mecanismo de control que permite verificar las acciones y decisiones, así como el fundamento de las mismas, que adopta la autoridad. La protección de datos por su parte, se constituye como un atributo inherente a toda persona que busca resguardar su privacidad e intimidad, configurándose como una garantía no solo para que un tercero no pueda interferir en su información o datos, sino también para que el titular de los datos pueda controlar sus datos y conocer quién los tiene y para qué los emplea.
b) La experiencia comparada de manera mayoritaria configura autoridades de control que se estructuran bajo el modelo único que solo regula y promueve la protección de datos de carácter personal. Así ocurre con los países de la OCDE y también de la UE, en este último caso, de los 28 países analizados, incluyendo para estos efectos el Reino Unido, 22 configuran sus agencias bajo el modelo único. A nivel latinoamericano, si bien la diferencia es menor, las legislaciones más recientes como Brasil y Ecuador, han estructurados entidades que solo regulan y promueven el derecho a la protección de datos.
c) También es importante considerar que a nivel europeo tanto la Carta de Derechos Fundamentales como el RGPD establecen un mandato a los países de la Unión Europea para configurar autoridades de control en materia de protección de datos. Mandato que la normativa europea no consagra en el caso de una institucionalidad para la regulación y promoción del derecho de acceso a la información pública.
d) Siguiendo con la experiencia comparada, en la mayoría de los países en que existe un modelo mixto, las entidades o agencias de control primero han regulado exclusivamente la protección de datos personales y luego, a través de reformas institucionales, se les ha adicionado la función de tutelar también el derecho de acceso a la información pública. Ese es el caso por ejemplo de Australia con la *Office of the Australian Information Comissioner OAIC*, cuya ley de 1998 le asignó competencias en materia de protección de datos personales y luego en el año 2010 se le asignaron funciones en materia de derecho de

acceso a la información pública. Los mismo ocurre con el Reino Unido, ya que la *Information Commissioner´s Office ICO*, asume la protección de datos personales en el año 1998 con la *Data Protection Act*, la que es modificada en el año 2004 por la *Freedom of Infromation Act and data protection Act* asumiendo el sistema mixto. A nivel latinoamericano ocurre algo similar[754], Argentina primero crea la Dirección Nacional de Protección de Datos reglamentada por el Decreto N° 1558, del año 2001, y luego en el año 2016, mediante la Ley N° 27.275 crea la Agencia de Acceso a la Información Pública que se configura en un sistema mixto. Así también ocurre en Perú, que primero crea la Dirección de Protección de Datos y luego la Dirección de Transparencia y Acceso a la Información, adscribiendo ambas al Ministerio de Justicia-Dirección General de Transparencia, Acceso a la información y Protección de Datos. La excepción es México, en donde el IFAI (Instituto Federal de Acceso a la Información) inició su labor en la promoción y protección del derecho de acceso, asumiendo en la actualidad la protección de datos personales, con lo que cambió su denominación a Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales ("INAI").

e) El CPLT en Chile tiene una tradición de más de diez años en la regulación y promoción del acceso a la información pública, lo que implica que existe una experiencia y hasta una inercia institucional en ese sentido. El adicionar la regulación de la protección de datos a dicho organismo puede salir incluso más costoso que la creación de una nueva autoridad de control para la protección de datos, no solo porque habrá que reestructurar su institucionalidad completa, hasta ahora solo diseñada para el derecho de acceso a la información pública, delimitando claramente su ámbito de actuación., En este sentido hay que recordar que el CPLT solo actúa sobre los organismos públicos, y el control del tratamiento de datos de carácter personal de manera muy importante también se realiza por entidades privadas. Pero incluso más, hoy los consejeros del CPLT no tienen dedicación exclusiva en el ejercicio de sus funciones, pudiendo desempeñarse en el quehacer privado, cuestión que indudablemente deberá cambiar si se opta por el modelo mixto.
f) En el sistema chileno, los órganos de control o lo que en la experiencia comparada se denominan las agencias regulatorias independientes, tienen un alto grado de especialización, encontrándose circunscrito su ámbito de intervención sobre un mercado, industria o interés específico y general. En este caso, el interés específico a regular y promover es la protección de datos de carácter personal y, es general porque consideraría tanto el tratamiento de datos que realicen entidades públicas como privadas. Así da cuenta la revisión efectuada a 22 agencias regulatorias.

[754]La excepción la representa México mediante el Instituto Nacional de Acceso a la Información y Protección de Datos, que primero abordó el acceso a la información pública y luego la protección de datos de carácter personal.

Argumentos a favor de un órgano colegiado

En relación a si la autoridad de control debe configurarse como un órgano colegiado o pluripersonal, es posible sistematizar los siguientes argumentos:

a) La regulación y promoción de la protección de datos pueden ser mejor desarrolladas a través de órganos colegiados, por cuanto facilita que las decisiones sean compartidas. Un Consejo u órgano colegiado compartiría la toma de decisión y permitiría la promoción de acuerdos mayoritarios o consensuados.

b) Los órganos colegiados favorecen más el debate técnico, la búsqueda de soluciones equilibradas y por consenso que tengan en cuenta los distintos intereses en juego. En efecto, la integración en la instancia decisional de dos o más personas promovería el debate y la reflexión fundada sobre las cuestiones a resolver.

c) Bajo ciertas condiciones un modelo de comisión o colegiado reduce el riesgo de captura regulatoria y fortalece la toma de decisiones. Una autoridad colegiada tiene más memoria institucional cuando el reemplazo es escalonado. Debido a esto, los cambios en la instancia colegiada son menos costosos y con menor probabilidad de modificar completamente el trabajo del regulador. Este modelo puede alejar a la institución del proceso político, por ejemplo, el nombramiento puede ir más allá de los periodos presidenciales o escalonar dicho nombramiento.

d) En términos generales, los modelos corporativos o colegiados tienen características más flexibles para impulsar la rendición de cuentas, la transparencia, efectividad, integridad e independencia del regulador.

Argumentos a favor de un órgano unipersonal

a) Los órganos cuyo gobierno superior es colegiado pueden ralentizar las decisiones y generar más espacio para la burocracia interna, diluyendo las responsabilidades y desincentivado la rendición de cuentas.

b) En contraste, una autoridad única puede ser más adaptable a los cambios de la industria y su capacidad de respuesta más rápida. La captura regulatoria es más desafiante cuando hay un solo miembro, pero la fortaleza institucional del ministerio principal puede brindar su apoyo en este asunto.

c) En el contexto Iberoamericano, la mayoría (5) de las agencias encargadas de la protección de datos se estructuran con una autoridad de control unipersonal, que es también el modelo que mayoritariamente siguen las agencias de los Estados miembros de la UE.

d) En la experiencia chilena, la que fue revisada en páginas anteriores en esta investigación, de las 22 agencias reguladoras independientes chilenas, 17 se estructuran bajo una autoridad unipersonal y solo 5 se constituyen bajo una autoridad colegiada. Tendencia que se mantiene en los últimos años como ocurre con el diseño y creación de la Superintendencia de Casinos de Juegos (2005); la Superintendencia del Medio Ambiente (2010), la Superintendencia de Insolvencia y Re-emprendimiento (2014) y la Superintendencia de Educación Superior (2018).

Como ya se analizó, en la experiencia comparada no existe un sistema preferente para la instalación de una autoridad de control en materia de protección de datos, una instancia colegiada o una autoridad unipersonal son perfectamente competentes para ejercer su función, lo relevante es su independencia y las atribuciones, poderes y recursos con los que cuenten para tutelar la protección de datos de carácter personal, por lo que en definitiva su diseño institucional dependerá de la tradición administrativa, la eficacia y eficiencia que uno u otro sistema, colegiado o unipersonal, haya demostrado en el respectivo Estado donde se pretenda instalar.

Propuesta

La propuesta que se formula en la presente investigación doctoral es la configuración de una Autoridad de Control de protección de datos personales bajo lo que se ha denominado el modelo único, es decir que regule y promueva exclusivamente el derecho a la protección de datos de carácter personal y que se estructure con una autoridad unipersonal. Esta entidad se denominaría Agencia Nacional de Protección de Datos, la que estará asesorada por una instancia colegida de carácter consultivo denominado Consejo Consultivo para la Protección de Datos. Este Consejo se conformará por representantes de otros poderes del Estado, autoridades independientes con competencias limítrofes, así como con miembros de la sociedad civil y de la academia, vinculados y conocedores de la protección de datos.

CONCLUSIONES

Finalizado el desarrollo de toda esta investigación se presentarán a continuación las principales conclusiones de sus distintas etapas, las que sustentan la propuesta de generar una institucionalidad que regule y promueva de manera exclusiva y excluyente la protección de datos de carácter personal en el ordenamiento jurídico chileno, bajo el diseño de una autoridad única de control unipersonal e independiente.

La exposición de las conclusiones se dividirá en dos partes, la primera para abordar las consideraciones finales más relevantes expuestas en cada uno de los capítulos de esta investigación y la segunda para señalar las conclusiones generales que se derivan de un trabajo reflexivo y de deliberación que propone la institucionalización de la protección de datos para Chile.

Primera Parte

1. La dignidad es el sustento de los derechos fundamentales que permiten concretar y satisfacer las necesidades de la persona en el ámbito moral y es por esa relación que la doctrina clásica ha distinguido los derechos de la personalidad, tales como el derecho al honor, el derecho a la intimidad, el derecho al respeto y protección a la vida privada, la libertad de conciencia y más recientemente (especialmente en el caso chileno) el derecho a la protección de datos personales. Es decir, son derechos que el individuo tiene por él solo, pero también por el significativo hecho de ser una persona.

2. La protección de datos personales surge y se desarrolla relacionada con el derecho a la intimidad y, en el caso del ordenamiento jurídico chileno, con el derecho a la protección a la vida privada. Sin embargo, el vertiginoso desarrollo de las tecnologías de la información, así como la relevancia del almacenamiento de los datos y su tratamiento tanto al interior de los Estados, en los sectores públicos y privados, como su transferencia a otros países, han impulsado desde hace ya varias décadas la configuración de un nuevo derecho fundamental con independencia y autonomía propia.

3. Como se ha señalado, la privacidad es más amplia que la intimidad, esta última se refiere a los ámbitos más reservados de la persona como es su domicilio, el ámbito familiar y en aquellos momentos y lugares en donde expresa sus pareceres y sentir. En cambio, la privacidad, al ser más amplia, considera un conjunto de aspectos de la persona que aislados pueden carecer de significación o relevancia, pero que ordenados sistémicamente pueden arrojar la identificación de una persona, la que tiene derecho a mantener en reserva dichos aspectos que le individualizan.

4. Europa, mucho antes que Latinoamérica y Chile, afrontó la tutela de los datos personales. Especial importancia tiene el Convenio 108, del 28 de enero 1981 para la Protección de las Personas respecto del Tratamiento Automatizado de Datos de Carácter Personal del Consejo de Europa al que pertenecen 46 países del ámbito regional europeo y que realiza

unas funciones similares a la Organización de Estados Americanos en lo relativo a la protección de derechos fundamentales.

5. En la Unión Europea se deben citar las Resoluciones (73)22, del 26 de septiembre de 1973 sobre la protección de la vida privada de las personas físicas respecto de los bancos de datos electrónicos en el sector privado, y la (74)29, de 20 de septiembre de 1974, sobre la protección de la vida privada de las personas físicas respecto de los bancos de datos electrónicos en el sector público. Posteriormente la Directiva 95/46/CE, instaba a los estados de la Unión Europea a regular el tratamiento de los datos personales de los ciudadanos europeos. La aprobación primero, y luego la entrada en vigor del Reglamento General de Protección de Datos de la UE (RGPD), no solo reforzó la uniformidad europea, sino que generó un efecto expansivo, influyendo también en otras latitudes, contribuyendo a consolidar la protección de datos personales como derecho fundamental, reconocido constitucionalmente en otros países, como ocurrió en Chile en junio del año 2018.

6. La Constitución Española (CE) en el apartado 4º del artículo 18 establece que "la Ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de los derechos". A partir de una referencia a los peligros que la informática supone para los derechos y libertades de las personas, se va a desarrollar un derecho fundamental con el apoyo del Convenio 108, la Directiva Europea 95/46/CE y la jurisprudencia constitucional que se regula en tres sucesivas Leyes Orgánicas: la 5/1992, la 15/1999 y la 3/2018.

7. El artículo 18 de la Constitución Española no se refiere al derecho a la privacidad, sino que se vincula con el derecho al honor, a la intimidad personal y a la propia imagen, a la inviolabilidad del domicilio y al secreto de las comunicaciones. Se trata de derechos fundamentales de la personalidad que se relacionan estrechamente, por cuanto abordan ámbitos privados de la persona del que están excluidas las demás, correspondiendo a cada cual compartir o no los datos que pueden afectar a su dignidad.

8. Los medios informáticos tienen la capacidad de archivar una cantidad ilimitada de información, a la que después se puede acceder fácil y rápidamente. Así ya lo declaraba el Tribunal Constitucional Federal Alemán, en su sentencia del 15 de diciembre de 1983: "Los procesos de decisión ya no se pueden retrotraer como antiguamente a registros y documentos compilados manualmente; antes bien, hoy día, gracias a la ayuda de la elaboración automática de datos, la información individual sobre circunstancias personales u objetivas de una persona determinada o, en su caso, determinable son técnicamente hablando acumulables sin límite alguno y en cualquier momento se pueden recabar en cuestión de segundos, cualquiera que sea la distancia".

9. Hace no tantos años atrás, la privacidad y la esfera personal de cada individuo estaban protegidas por el tiempo y por el espacio; en efecto, el transcurso del tiempo permitía que los hechos ocurridos se olvidaran evitando el desarrollo de una historia lineal e ininterrumpida de la persona; a su vez la distancia impedía que se conocieran los hechos ocurridos en un lugar distinto. Esos límites han desaparecido por las tecnologías de la información: la informática, las telecomunicaciones y la inteligencia artificial, lo que permite un conocimiento completo del individuo, al que solo debe de tener acceso él

mismo o, aquellos a los que él autorice o cuando exista una causa justificada de interés público. El acceso y procesamiento a los datos y a la información ordenada y sistematizada puede dibujar un determinado perfil de la persona o incluso incidir en su reputación o fama.

10. Incluso esa información y su tratamiento informático es utilizado como técnica de acumulación para controlar o incidir en determinados comportamientos ideológicos y políticos, lo que supondría un grave atentado a los derechos fundamentales, por lo que es imprescindible establecer sistemas de garantías que tutelen y protejan a las personas.

11. La protección de datos se configura como un derecho fundamental autónomo, con una configuración propia que busca resguardar a las personas físicas respecto de su información personal que se contiene en diversas bases de datos y que aceleradamente se propaga con el vertiginoso desarrollo de las telecomunicaciones, la informática y la inteligencia artificial.

12. La señalada autonomía de la protección de datos no es absoluta, por lo que debe ponderarse con otros derechos. Por ello, en ciertos y determinados casos, por ejemplo, en materia penal, las autoridades respectivas están habilitadas para acceder a los datos de los titulares o interesados (nombre, apellido y dirección) por un lapso específico de tiempo y circunscrito a la prevención, investigación, descubrimiento y persecución de delitos.

13. De la configuración del derecho a la protección de datos surgen los denominados derechos o facultades ARCO: acceso, rectificación, cancelación y oposición, hoy complementados por los derechos de supresión u olvido, de portabilidad y de límites al tratamiento, que algunos han denominado derechos ARCO – PLUS.

14. Si bien el derecho al olvido en el contexto latinoamericano tiene un incipiente reconocimiento, en el ámbito europeo ha tenido un rápido y creciente progreso, primero con la sentencia del Tribunal de Justicia de la Unión Europea (TJUE) del 13 de mayo del 2014, caso Mario Costeja González y Agencia Española de protección de Datos (AEPD) versus Google Spain y Google Inc., donde se le da al derecho a supresión un sentido y alcance mayor en un entorno virtual, como es la obligación de suprimir u olvidar para todo responsable del tratamiento de datos que en determinadas circunstancias afecte al titular de los mismo, en el contexto de los denominados motores de búsqueda en internet. Derecho que se incorporará posteriormente en el RGPD que lo reconoce expresamente en el artículo 17.

15. De la jurisprudencia revisada del Tribunal de Justicia de la Unión Europea (TJUE) relacionada con la protección de datos personales, es posible también extraer importantes conclusiones generales, que contribuyen a determinar el contenido y alcance de este derecho fundamental:

    a) La noción de “responsable del tratamiento” a la que alude la normativa europea, primero contenida en la Directiva 95/46/CE y en la actualidad en el RGPD, debe ser entendida en sentido amplio, por cuanto esa expresión comprendería, según las sentencias analizadas, tanto al administrador de una página web o de una red social,

a los proveedores de la misma, a una comunidad religiosa que en actividades de predicación puerta a puerta recoge datos de los interesados, a un gestor de un motor de búsqueda, o incluso, a una comunidad de copropietarios de un edificio que instalan cámaras de videovigilancia.

b) En lo referido a las competencias de la autoridad de control en protección de datos, la jurisprudencia analizada concluye que dicha entidad, en el ámbito europeo, tiene la facultad para regular las sucursales en Europa de las empresas extranjeras que realicen tratamiento de datos personales o actividades afines a ello (publicidad o promoción de ciertos productos), aun cuando la matriz de dicha empresa se encuentre ubicada fuera de un Estado miembro de la Unión. De igual forma la autoridad de control puede fiscalizar de manera autónoma e independiente de la autoridad de control local, a una entidad o empresa cuya matriz, este establecida en su mismo territorio, aun cuando el responsable del tratamiento de los datos tenga su domicilio en otro Estado miembro.
c) Sobre el principio de ponderación, el TJUE ha señalado que la obligación de retirar enlaces que traten datos personales incluye a los gestores de un motor de búsqueda, sin perjuicio de las excepciones que la normativa sobre protección de datos establezca, ya sea la Directiva 95/46/CE o el RGPD, compatibilizando dicha obligación con la Carta de Derechos Fundamentales de la Unión Europea CDFUE, debiendo ponderarse, con todos los antecedentes pertinentes, el eventual conflicto entre la protección de datos de carácter personal y la protección a la vida privada y familiar por una parte y, por la otra, la libertad de expresión e información.
d) Coincidente con el punto anterior, la intensidad con que se lesionen o afecten los derechos y libertades del interesado constituye un elemento esencial del ejercicio de ponderación, o de ponderación caso por caso, debiendo considerarse la naturaleza de los datos personales en cuestión, en particular el carácter potencialmente sensible de los mismos, así como la naturaleza y el modo concreto de su tratamiento, en particular el número de personas que tienen acceso a ellos y el modo en que acceden.
e) Sobre el consentimiento del interesado, al que aluden tanto la Directiva 95/46/CE como el RGPD, el TJUE ha señalado que este no es válido cuando el almacenamiento de información o el acceso a la información ya almacenada en el equipo terminal del usuario de un sitio de Internet a través de las denominadas *cookies*, se autoriza mediante una casilla marcada por defecto de la que el usuario debe retirar la marca en caso de que no desee prestar su consentimiento, debiendo por consiguiente, dicho consentimiento ser especifico e inequívoco.
f) Finalmente, sobre el interés legítimo como una excepción al tratamiento de datos de carácter personal, el TJUE ha resuelto que debe garantizar la seguridad de los bienes y de las personas, y prevenir la comisión de delitos, objetivo que no puede alcanzarse razonablemente de manera tan eficaz por otros medios menos atentatorios respecto de los derechos y libertades fundamentales de los interesados, consagrados en la CDFUE.

16. Revisados los ordenamientos jurídicos latinoamericanos en protección de datos, es posible colegir las siguientes consideraciones:

a) La regulación de la protección de datos personales en las constituciones latinoamericanas es diversa, y en muchos casos más bien deriva de una

interpretación o extensión de los derechos a la intimidad, vida privada, honra o imagen que de una mención explícita que lo reconozca. En otros casos, más que una referencia o regulación a la protección de datos se refieren al habeas data, como un mecanismo o acción para tutelar el derecho a la protección de datos, aun cuando este no tenga un tratamiento expreso. En otras constituciones no hay referencia explícita alguna ni a la protección de datos, ni al habeas data, no obstante, su regulación queda radicada en el ámbito legislativo.

b) Cualquiera que sea el orden o estructura como se configuren las leyes sobre protección de datos latinoamericanas, ya sea en títulos, capítulos o secciones, en general se distinguen como elementos centrales: una conceptualización de términos en donde destacan las definiciones de datos personales y datos sensibles; los principios en que debe sustentarse el tratamiento de datos; los derechos de los titulares de los datos; la transferencia de datos; la autoridad de control en la materia; y la acción o procedimiento de tutela, así como las sanciones a que se verán expuestas las entidades públicas y privadas que no cumplan con sus disposiciones. Y si bien hay países que no tienen una legislación específica en materia de protección de datos, como es el caso de El Salvador, Honduras o Guatemala, es la legislación sobre transparencia y acceso a la información pública la que regula aspectos relacionados con la protección de datos.

c) También de la revisión latinoamericana se concluye que Argentina y Uruguay son, hasta ahora, los únicos países reconocidos por la Comisión Europea con estándares adecuados en materia de protección de datos personales. Por delante de México, el que aparece con una robusta legislación en protección de datos, normando tanto el tratamiento que de estos hacen organismos públicos que se denominan sujetos obligados, como instituciones privadas. También resulta llamativo en la legislación mexicana que el consentimiento del titular de los datos, en determinadas circunstancias pueda ser tácito, salvo en el caso del tratamiento de los denominados datos sensibles, el que siempre deberá ser expreso.

d) Otro aspecto es que la mayoría de los países latinoamericanos regula a nivel constitucional una acción judicial para tutelar la protección de datos, dicha acción es el denominado *habeas data*. En efecto, a diferencia de los países europeos, que fijaron como mecanismo de regulación y promoción para la protección de datos personales el establecimiento de una autoridad de control en la materia, en Latinoamérica se ha utilizado un instrumento jurisdiccional, que precisamente es el *habeas data* y que está presente en las constituciones de Argentina (art. 43), Bolivia (art. 130), Brasil (art. 5° N°71), Ecuador (art. 92), Honduras (art. 182 N°2), Paraguay (art. 135), Perú (art. 200 N°3) y Republica Dominicana (art.70), por mencionar algunas.

e) Se observa que el RGPD ha influenciado fuertemente las legislaciones de la región, en especial las más recientes, como es el caso de la ley de protección de datos panameña que entró en vigor a partir de este año 2021 o la legislación brasilera en la materia, cuyo articulado completo entró en vigor en agosto del año 2021. Sin embargo, no todos los países de la región cuentan con autoridades de control independientes y radican la regulación y promoción de la protección de datos en unidades o instancias dependientes de los ministerios, como es el caso de Perú, a

través del Ministerio de Justicia, y Nicaragua, donde la regulación de la protección de datos está a cargo del Ministerio de Hacienda.

17. Un aspecto fundamental para la configuración de una agencia reguladora de la protección de datos a la que hace referencia el RGPD es su carácter autónomo o independiente. Dicho carácter no es solo una autonomía del ejecutivo o gobierno, sino también una independencia de los poderes políticos del Estado, evitando así una eventual captura de las fuerzas políticas sobre la Administración. El estándar, entonces, para las entidades que ejercen funciones de control, es lo que algunos autores han denominado una "neutralidad amplia", sacando, en este caso, la regulación y promoción de la protección de datos de carácter personal, de las decisiones que pudieran ser fluctuantes dependiendo de la influencia que determinadas fuerzas políticas o ciclos electorales ejerzan en momentos también determinados. Además, la independencia de las entidades de control encuentra también sustento en las funciones de supervisión, regulación y sanción que deben ejercer. En efecto, la independencia tiene su causal o motivo en que dichas funciones son eminentemente jurídicas y no políticas, por lo que cuando una entidad de la administración lleva a cabo una actividad de regulación, esta no debe efectuarse atendiendo a criterios políticos, sino exclusivamente técnicos. Y especialmente se expresa esa independencia en la inamovilidad, durante un periodo determinado de tiempo de la o las instancias decisorias y de dirección que tengan.

18. A lo largo de esta investigación se ha confirmado que para tutelar adecuadamente el derecho de protección a los datos personales existen diversos mecanismos, uno de ellos es el establecimiento de órganos de control y concretamente el de la configuración de agencias o entidades independientes, las que como se ha visto pueden estructurarse de diversas formas.

Segunda Parte

19. En el caso chileno se ha argumentado que la reconfiguración de la protección de datos tendría entre otras razones, la de cumplir con las exigencias formuladas por la OCDE para perfilarse como un país con un sistema seguro en el tratamiento de datos personales, especialmente en lo referido a la transferencia internacional de datos, sin embargo, esas afirmaciones parecen olvidar que Chile pertenece tanto a la Organización de las Naciones Unidas como a la Organización de Estados Americanos. La primera de ellas ya ha emitido Directrices para la regulación de los archivos de datos personales informatizados mediante la Resolución 45/95 de la Asamblea General de 14 de diciembre de 1990 y luego a través de la Resolución A/C.3/68/L.45/Rev.1 sobre el Derecho a la Privacidad en la Era Digital del año 2013.

20. A su vez, la Organización de Estados Americanos ha regulado la materia tanto a través de la Resolución AG/RES. 2842 (XLIV-O/14) sobre acceso a la información pública y protección de datos personales, estableciendo además los Principios de la OEA sobre la Privacidad y la Protección de Datos Personales.

21. A mayor abundamiento, un tratado vigente, el Acuerdo por el que se establece una Asociación entre la Comunidad Europea y sus Estados miembros, por una parte, y la República de Chile, por otra, publicado en el Decreto 28 de 2003, del Ministerio de Relaciones Exteriores, dice textualmente en el artículo 202 "Las Partes acuerdan otorgar un elevado nivel de protección al procesamiento de datos personales y de otra índole, compatible con las más altas normas internacionales". Por lo expuesto se puede concluir que Chile ya ha asumido compromisos internacionales en materia de regulación y tratamiento de datos personales.

22. El derecho a la protección de datos no es la otra cara del derecho al acceso a la información pública. La transparencia y el acceso a la información son líneas de acción que se han desarrollado en base a la necesidad creciente de los Estados de contar con herramientas para luchar contra la corrupción y de los ciudadanos en participar en los recursos informativos públicos. En cambio, el derecho fundamental a la protección de datos es un derecho que incide en la tutela de otros derechos fundamentales de las personas y aunque posea una facultad de acceso a los datos personales que podría identificarse con el derecho de acceso, en realidad ambos derechos son diferentes.

23. Para la institucionalización de la protección de datos en Chile, resulta indispensable considerar el concepto de autonomía en la estructura de la Administración del Estado, que es una noción indeterminada, ya que ni la Constitución ni las leyes la explicitan, no obstante, se refieren a ella al configurar ciertos órganos como autónomos constitucionalmente o autónomos legalmente. En cualquier caso, como se explicó en el desarrollo de esta investigación, la autonomía tiene relación con la independencia que la entidad o el titular de ésta tienen frente al Presidente de la República y otras autoridades públicas. Existiendo en el sistema chileno entidades que tienen más independencia de aquel, como la Contraloría General de la República o el Banco Central, y, otros que tienen menos independencia del Presidente, como el caso del Servicio Nacional de Aduanas o las Superintendencias.

24. Si se analizan los órganos con autonomía, se podrá concluir que estos en muchos casos tienen su antecedente en demandas sociales que han debido ser canalizadas institucionalmente, por ejemplo, el Consejo para la Transparencia, órgano legalmente autónomo que surge de las reivindicaciones sociales por obtener información de entidades públicas, demanda que tuvo su expresión en el caso ante la Corte Interamericana de DD. HH "Claude Reyes y otros versus Chile". En este sentido parece adecuado que la configuración de una entidad de control que institucionalice la protección de datos personales en Chile se configure como una entidad con autonomía sea legal o constitucional, con altos niveles de independencia del poder ejecutivo o Presidente de la República y que por lo tanto acoja la creciente demanda ciudadana por tutelar la protección de los datos de las personas.

25. Una Autoridad de Control debe tener las capacidades suficientes para asegurar la tutela y defensa del derecho fundamental a la protección de datos, otorgando un tratamiento igualitario al sector público y al sector privado, garantizando tanto el tráfico internacional como el flujo transfronterizo de datos, insertándose armónicamente en la estructura administrativa, siendo reconocida y validada por la ciudadanía.

26. Lo que el presente trabajo de investigación propone es separar las competencias de regulación y promoción de la protección de datos, de las relacionadas con el derecho de acceso a la información pública. Propuesta que difiere del proyecto de ley actualmente en discusión, en primer trámite constitucional, en el Senado chileno. En este sentido la composición que tiene actualmente el CPLT hace difícil que este sea un órgano de control en materia de protección de datos, entre otras razones por que su actual configuración no regula adecuadamente los eventuales conflictos de interés que puedan tener, en el sentido de que los consejeros no ejercen sus funciones de manera exclusiva, pudiendo ser representantes y directores de empresas o entidades privadas que hacen tratamiento de datos personales.

27. El separar las funciones de protección de datos y de acceso a la información pública requiere como elemento central, la debida coordinación entre los órganos del Estado intervinientes, en efecto, las entidades involucradas deben propender a un alto grado de interoperabilidad y coherencia de modo de evitar contradicciones en la información almacenada y reiteración de requerimientos de información o documentos a los titulares de datos. Ejemplo a seguir en esta materia en Chile sería el caso español que a través de la ley regula la debida coordinación entre la protección de datos, a cargo de la Agencia Española de Protección de Datos y el derecho de acceso a la información pública, a cargo del Consejo para la Transparencia y Buen Gobierno. Así, se establece en la Disposición adicional quinta de la Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno, que en lo relativo a la "Colaboración con la Agencia Española de Protección de Datos", "El Consejo de Transparencia y Buen Gobierno y la Agencia Española de Protección de Datos adoptarán conjuntamente los criterios de aplicación, en su ámbito de actuación, de las reglas contenidas en la propia ley, en particular en lo que respecta a la ponderación del interés público en el acceso a la información y la garantía de los derechos de los interesados cuyos datos se contuviesen en la misma…".

28. Entre los argumentos para proponer este modelo institucional, que como se señaló a lo largo del presente trabajo, denominamos modelo único (en contraposición al modelo mixto que es aquel en que la autoridad de control en protección de datos además regula el derecho de acceso a la información pública) es posible configurar diversos argumentos que se suman a los ya señalados, desde la perspectiva de los principios, funciones, mercados y conflictos de interés.

    a) En efecto, en relación con los *Principios*, como se ha expuesto a lo largo de todo este trabajo investigativo, el Acceso a la Información y la Protección de Datos tienen orígenes y focos muy distintos e incluso contradictorios: la protección busca tutelar la información de cada persona resguardando su identidad, permitiendo además que cada titular pueda disponer libremente de la información que le incumbe. En cambio, la transparencia persigue poner freno a la corrupción y es un instrumento que promueve la probidad especialmente en el quehacer público;
    b) En cuanto a las *Funciones* de una y otra, estas también son muy diversas. La función de la Protección de Datos está orientada hacia la seguridad y tratamiento de información en procesos de alta complejidad. Tanto los procesos como los perfiles

profesionales que se requieren son muy distintos a lo que se requiere para el Acceso a la Información, donde el foco está en la adopción de buenas prácticas en el sector público y no en la fiscalización de procesos complejos.

c) Respecto de los *Mercados*: El ámbito principal de la Protección de Datos está en el sector privado. Es en este sector donde se encontrarán los principales detractores del Consejo en su función, donde tendrá que lidiar con industrias enteras dedicadas al tratamiento de la información personal de terceros y donde se presentarán los mayores desafíos a la regulación. El mercado del Acceso a la Información es el sector público y los dilemas entre ambas están orientados a la primacía de un derecho sobre el otro y a la construcción de dicha normativa;
d) Sobre los *Conflictos de intereses*: La institucionalidad ligada al Acceso a la Información está pensada principalmente en su independencia frente al Poder Ejecutivo. En el caso de la Protección de Datos los principales conflictos de intereses se darán con el sector privado, por ende, la contraposición de intereses se vuelve mucho más compleja.

29. En el sistema chileno, las agencias regulatorias independientes tienen un alto grado de especialización, encontrándose restringido su ámbito de intervención sobre un mercado, industria o interés específico. Su diseño institucional responde al de un servicio público funcionalmente descentralizado, en la mayoría de los casos con una autoridad unipersonal que las dirige, designada por el ejecutivo, observándose una tendencia en los últimos años a que el proceso de selección de dicha autoridad se realice a través del Sistema de Alta Dirección Pública (SADP).

30. Así entonces, para la estructuración de una autoridad de control para la protección de datos en Chile, resulta indispensable concebirla como una agencia regulatoria independiente con altos estándares de especialización y con un diseño de gobierno, sea unipersonal o colegiado, que no se vea afectado por los cambios de gobierno, que goce de inamovilidad y que las causales de remoción estén taxativamente establecidas en la respectiva legislación. En este sentido, y considerando la revisión realizada, pareciera que lo más aconsejable sobre su ámbito competencial es que este sea acotado a salvaguardar un interés específico o regular un sector económico o industria más bien determinado, por lo que no parece lo más conveniente que al Consejo para la Transparencia (CPLT) se le asigne la función de tutelar la protección de datos de carácter personal, por cuanto desde su creación sus funciones han estado focalizadas en regular y promover la transparencia y el acceso a la información público.

31. En la experiencia chilena, la que fue revisada en el Capítulo V de esta investigación, de las 22 agencias reguladoras independientes 17 se estructuran bajo una autoridad unipersonal y solo 5 se constituyen bajo una autoridad colegiada. Tendencia que se mantiene en los últimos años como ocurre con el diseño y creación de la Superintendencia de Casinos de Juegos (2005); la Superintendencia del Medio Ambiente (2010), la Superintendencia de Insolvencia y Re-emprendimiento (2014) y la Superintendencia de Educación Superior (2018).

32. En el proceso de selección del titular de la autoridad de control, será importante transparentar las postulaciones, por ejemplo, a través de audiencias públicas u oposición de antecedentes donde los postulantes presenten los lineamientos que enfatizarán en su eventual gestión y puedan ser consultados por la entidad llamada a su selección.

33. A lo ya señalado sobre la autoridad de control, se sugiere considerar el fortalecimiento de una acción o recurso jurisdiccional, que, si bien está presente en la aún vigente ley 19.628 sobre protección a la vida privada, en los hechos ha resultado inaplicable. El habeas data, establecido en el artículo 16 de la señalada ley, debe ser reconfigurado y reconocido constitucionalmente, como ocurre en la mayoría de las Cartas latinoamericanas, como un coadyuvante al establecimiento de una autoridad de control que garantice, regule y promueva la protección de datos de carácter personal.

34. Considerando el *momentum* constitucional por el que atraviesa Chile, existe una oportunidad inigualable para repensar la protección de datos y formular una institucionalidad que desde la nueva Constitución asegure su adecuada promoción y tutela. Para lo cual se propone:

    a) Consagrar de manera expresa la protección de datos personales en el catálogo de derechos fundamentales y, además hacer referencia a su contenido estableciendo los denominados derechos ARCO.
    b) Disponer que a través de la respectiva ley se estructurará una entidad o autoridad de control encargada no solo de proteger y fiscalizar tanto a instituciones públicas como privadas en el cumplimiento efectivo del respeto a la protección de datos personales como derecho fundamental, sino además se encargue de su promoción y del desarrollo de acciones preventivas para su adecuado resguardo.
    c) Incorporar en la nueva Carta Política el habeas data como una acción que complemente la tutela de la autoridad de control para resguardar el derecho a la protección de datos personales y sus diferentes manifestaciones (derechos ARCO).

35. Finalmente, de la revisión de cómo se estructuran las autoridades de control para la protección de datos en la experiencia comparada, es posible vislumbrar futuras líneas de investigación especialmente relevantes en el ámbito latinoamericano, que por ejemplo promuevan directrices comunes para su regulación; un incipiente intento de aquello son los Estándares de Protección de Datos de la Red Iberoamericana de Protección de Datos, que aun cuando constituyen normas de *soft law*, son un primer intento para estandarizar criterios, lo que es y será una necesidad aún más creciente debido a la transferencia internacional y transfronteriza de datos.

Por último, durante todo este trabajo de investigación ha quedado de manifiesto la inequívoca naturaleza jurídica de la protección de datos de carácter personal, que se configura como un derecho fundamental de la mayor relevancia, derivado del creciente y vertiginoso desarrollo de la informática, las telecomunicaciones, la inteligencia artificial y el *big data* que permiten almacenar, tratar y trasmitir una infinidad de datos. Con ello es posible llegar a influir o incluso

manipular el comportamiento de los individuos y, a la vez gestionar transacciones e interacciones sin que en muchos casos ni siquiera tengamos la debida conciencia de aquello. La nueva Era en la que estamos inmersos ha sido inundada por el desarrollo tecnológico, hasta el punto que nunca antes la Humanidad había sido capaz de recoger, procesar y almacenar tal nivel de información y, a su vez compartirla o tratarla a través de transmisiones remotas que, si bien acortan las distancias y el tiempo, también despersonalizan y automatizan las relaciones del ser humano.

Chile atraviesa por un proceso único en toda su historia republicana, por primera vez en más de 210 años los ciudadanos eligieron a representantes que redactarán una nueva Constitución para el país. El fortalecimiento de nuevos derechos, tales como los derechos digitales o la reconfiguración y fortalecimiento de otros ya existentes como el respeto y protección a la vida privada o el derecho a la protección de datos, será parte esencial de la redacción del nuevo texto político, lo que representa una oportunidad sin igual para configurar un rediseño institucional que establezca una Autoridad de Control que institucionalmente garantice la protección de datos de carácter personal.

La investigación doctoral que aquí se presenta propone la instalación de una institucionalidad que asegure y promueva el derecho a la protección de datos de manera exclusiva y que contribuya a la generación de una conciencia en pos de la privacidad y de la importancia de resguardar la información de todas las personas.

BIBLIOGRAFÍA

Abad Alcalá L., (2020). *Las libertades informativas en el ámbito internacional*. Dykinson.

Agencia de los Derechos Fundamentales de la Unión Europea, (2010), "*Data Protection in the European Union: the role of National Data protection Autohorities*", Oficina de Publicaciones de la Unión Europea, Luxemburgo.

Aldunate Lizana, E., (2008), *"Derechos Fundamentales"*, Santiago, Legal Publishing.

Alexy, R., (2014), "Constitutional Rights and Proportionality," Revus, *Journal for constitutional theory and philosophy of law*, nº 22.

Álvarez Caro, M., (2015),"Derecho al Olvido en Internet: el nuevo paradigma de la privacidad en la era digital", Reus.

Álvarez Rigaudias, C., (2018), "Transferencias de datos personales a terceros países y organizaciones internacionales (artículos 44-50)", en "*El nuevo marco regulatorio de derivado del Reglamento Europeo de Protección de Datos. Adaptado al proyecto de Ley Orgánica de Protección de Datos de 10 de noviembre de 2017"*, coordinador José López Calvo, Boch, Barcelona.

Álvarez Rigaudias, C., (2019), "Transferencia de Datos Personales a terceros países y organizaciones internacionales (Artículos 44-50 del RGPD. Artículos 40-43 y disposición adicional quinta y decimotercera de la LOPDGDD)", La adaptación al nuevo marco de protección de datos tras el RGPD y la LOPDGDD", coordinador José López Calvo, Boch, Barcelona.

Alvarez Valenzuela, D. (2016), "Acceso a la Información Pública y Protección de Datos Personales. ¿Puede el Consejo para la Transparencia ser la Autoridad de Control en materia de Protección de Datos?", en Revista de Derecho de la Universidad Catolica del Norte. Año 23, N°1, 2016, pp. 51-79.

Anguita, P., (2007), "La protección de datos personales y el derecho a la vida privada, Régimen jurídico, jurisprudencia y Derecho comparado", Editorial Jurídica de Chile, Santiago.

Aparicio Salom, J., (2018), "*Derechos del Interesado*" (artículos 12-19), El nuevo marco regulatorio derivado del Reglamento Europeo de Protección de Datos. Adaptado al Proyecto de Ley Orgánica de Protección de Datos de 10 de noviembre de 2017, coordinador José López Calvo, Boch, Barcelona.

Aparicio Wilhelmi M. y Pisarello Prados G. (2013) "Los derechos humanos y sus garantías: nociones básicas". Universitat Oberta de Catalunya, pp.16-17.

Arrieta Cortes, R. (2019) "El nuevo entorno regulatorio de la protección de datos en Chile", en International Association of Privacy Professionals – IAPP. Ver en:

https://iapp.org/news/a/el-nuevo-entorno-regulatorio-de-la-proteccion-de-datos-personales-en-chile/

Araujo, L. y Serrano Nunes J., (2011), "*Curso de direito constitucional*". 15° ed. Säo Paulo, Editora Verbatim.

Balducci Romano, F., (2013), "The Right to the Protection of Personal Data: A New Fundamental Right of the European Union". Falta editorial.

Bawn, K., (1995), "Political control versus expertise: Congressional choices about administrative procedures", *American Political Science Review*, Vol. LXXXIX, n° 1.

Becher, J., (2004), "El individuo, las tecnologías de la información y los medios de comunicación de masas", en *Historia de la Humanidad, T. El Siglo XX. La Globalización de las culturas*, Editorial Planeta, 2004.

Berrocal Lanzarot A., (2019) "Estudio Jurídico-Crítico sobre la Ley Orgánica 2/2018, de 5 de Diciembre de Protección de Datos Personales y Garantías de Derechos Digitales", Reus, Madrid.

Blanco Antón, M., (2019), "Autoridades de Control Independientes (Arts. 51-59 RGPD). Autoridades de Protección de Datos (Arts. 44-59 y Disposición adicional cuarta LOPDGDD)", en *"La Adaptación al Nuevo Marco de Protección de Datos tras el RGPD y la LOPDGDD"*, Coordinador José López Calvo, Boch Wolters Kluwer.

Blanes Climent, M.A. *Blog de Transparencia y Gobierno Abierto – Transparency and Open Government* https://miguelangelblanes.com/

Bru Cuadrada, E., (2007), "La protección de datos en España y en la Unión Europea. Especial referencia a los mecanismos jurídicos de reacción frente a la vulnerabilidad del derecho a la intimidad", *Revista de los Estudios de Derecho y Ciencia Política (IDP)*, n°5.

Bush, A., (2013), "*The Regulation of Privacy, Handbook on the Politics of Regulation*", Edited by David Levi-Faur, E., Publishing Limited.

Camacho G (2014) La protección de datos como frontera del derecho de acceso a la información". Revista de Grestión Pública, vol. III. N°1, pp.73-93, p.81.

Carrillo, M., (2016), "Los ámbitos del derecho a la intimidad en la sociedad de la comunicación" en *Cuadernos y Debates* n° 248: El derecho a la privacidad en un nuevo entorno tecnológico. Madrid, Centro de Estudios Políticos y Constitucionales.

Cazurro Barahona, V., (2020), "Antecedentes y Fundamentos del Derecho a la Protección de Datos", Boch Editor, Barcelona.

Cerda A. (2003). "La autoridad de control en la legislación sobre protección frente al tratamiento de datos perdsonales". Santiago, Tesis para optar al grado de magister en Derecho Público, Universidad de Chile.

Cerda Silva, Alberto. (2011). El "nivel adecuado de protección" para las transferencias internacionales de datos personales desde la Unión Europea. *Revista de derecho (Valparaíso)*, (36), 327-356. https://dx.doi.org/10.4067/S0718-68512011000100009

Concepción Rodríguez J.L, (1996), "Honor, intimidad e imagen: un análisis jurisprudencial de la L.O 1/1982", Barcelona, Boch.

Conde Ortiz, C., (2005), "La Protección de datos personales. Un derecho autónomo con base en los conceptos de intimidad y privacidad", Madrid, Dykinson.

Contreras, P., (2020), "El derecho a la protección de datos personales y el reconocimiento de la autodeterminación informativa en la Constitución chilena", en *Revista de Estudios Constitucionales*, vol. 8, nº 2.

Contreras, Bordachard y Ortiz editores (2022) en *"Privacidad y protección de datos personales. Jurisprudencia seleccionada y comentada"* DER ediciones, Santiago de Chile,

Cordero Quinzacara, E., (2012), "La Admnistración del Estado en Chile", en *La Contraloría General de la República, 85 años de vida institucional* (1927-2012), ediciones Contraloría General de la República, Santiago de Chile.

Corredoira L. y Cotino Hueso, L. (coordinadores), (2013), "*Libertad de expresión e información en Internet: amenazas y protección de los derechos personales*, Madrid, Centro de Estudios Políticos y Constitucionales.

Cotino Hueso, L. y Valero Torrijos, J. (Coordinadores) (2010), *"Administración Electrónica"*. Ed. Tirant lo Blanch, Valencia.

Dadingo Guerra, A. (1996) " Sobre la aplicación extensiva de la institución de la responsabilidad patrimonial de la Administración a los daños sufridos por entidades públicas". Revista Española de Derecho Administrativo REDA, N° 92, p. 652.

Dávara Rodríguez, M., (2013), "*El derecho al olvido en internet*", La Ley, año XXXIV, n° 8137.

De Terwangne, C., (2012), "Privacidad en Internet y el derecho a ser olvidado/derecho al olvido", Monográfico, "VII Congreso Internacional Internet, Derecho y Política. Neutralidad de la red y otros retos para el futuro de Internet", *Revista D'Internet, Dret i Politica*, (IDP), n° 13.

Delgado Martín, J., (2019), "Reflexiones sobre la protección de datos personales en la Administración de Justicia", *Diario La Ley*, n° 9326, sección Tribuna, 21 de febrero.

Desantes, J., (1991), *"El Derecho Fundamental a la Intimidad"*, en Seminario "El derecho a la intimidad y a la vida privada y los medios de comunicación social", realizado el 28 de agosto de 1991 en el Centro de Estudios Públicos, Santiago de Chile.

Drake, P., (1989), "The money doctor in the Andes: the Kemmerer missions, 1923-1933", Duke, Duke University Press.

Espín Templado, E., (1991), "Fundamento y alcance del derecho fundamental a la inviolabilidad del domicilio", *Revista del Centro de Estudios Constitucionales*, nº 8, Madrid, España.

Fernández-Izquierdo, F., (2000), "La historia moderna y nuevas tecnologías de la información y las comunicaciones", *Cuadernos de Historia Moderna*, Vol. 24.

Frigerio Dattwyler, Catalina. (2018). Mecanismos de regulación de datos personales: una mirada desde el análisis económico del derecho. *Revista chilena de derecho y tecnología*, *7*(2), 45-80. https://dx.doi.org/10.5354/0719-2584.2018.50578

Frosini, V. (1988), "*Informática y Derecho*", trad. del italiano por Jorge Guerrero y Mariano Ayerra Redin, Bogotá. Temos.

Fuertes, M. (2019) "En defensa de la neutralidad en la Red" en *Otro Sí* . Colegio de Abogados de Madrid. Páginas 32-33

Gallimard, S., (2002), "Expertise, subversion, and bureaucratic discretion", *Journal of Law, Economics and Organization*, Vol. XVIII, n° 2.

Gamero Casado, E. (1997) "Las transformaciones del sistema de responsabilidad administrativa extracontractual". En *La responsabilidad patrimonial de los poderes públicos en el marco de la estructura territorial del Estado. III Jornadas d eestudio del Gabinte Jurídico de la Junta de Andalucia.* Granada: Comares.

García, A. L., (1984), "La Interpretación de la Constitución, Centro de Estudios Constitucionales", Madrid.

García, J. y Verdugo, S., (2010), "De las Superintendencias a las Agencias Regulatorias Independientes en Chile: Aspectos Constitucionales y de Diseño Regulatorio", *Actualidad Jurídica Universidad del Desarrollo*, vol. XXII.

García Mexia, P. (2019) "Los derechos digitales en la nueva ley de datos. ¿valor simbólico u operatividad real?" en *Otro Sí* . Colegio de Abogados de Madrid.

García San Miguel, L., (1992), "*Estudios sobre el derecho a la intimidad*", Alcalá de Henares, Madrid. Tecnos.

Garzón Valdés, E., (2015), "Lo íntimo, lo público y lo privado", en *Cuadernos de Transparencia*, n° 6, Instituto de Investigaciones Jurídicas, Universidad Nacional Autónoma de México.

Goig Martínez, J. M., Núñez Rivero, C., y Núñez Rivero, C. (2017*). Configuración del estado constitucional en España*. Dykinson.

Goig Martínez, J. M., Núñez Rivero, C. y Núñez Martínez M.A. (2019). *El sistema de fuentes del derecho constitucional en la jurisprudencia del tribunal constitucional español*. Universitas

Gonzalez Fuster, G., (2015), "The Emergence of Personal Data Protection as a Fundamental Rigth of the EU", Bruselas, Springer.

Gomes de Andrade, N., (2012), "El olvido: el derecho a ser diferente de uno mismo. Una reconsideración del derecho a ser olvidado", IDP, *Revista de Internet, Derecho y Política*, n° 13.

Greenwood, J. y Wilson, D., (1989), "*Public Administration in Britain Today*", Unwin Hyman, London, 2º ed.

Guerrero Picó, M., (2006), "El Impacto del Internet en el derecho fundamental a la protección de datos de carácter personal"; Sine loco, Thomson Civitas.

Hernández López, J., (2018), "Reglamento General del Protección de Datos. Incluye cronología, webgrafía, bibliografía e índice analítico", Valencia, Tirant lo Blanch.

Hubmann, H., (1967), "*Das Personlichkeitsrecht*", Colonia, 2° edición.

Hustinx, P., (2013) "EU Data Protection Law: The Review of Directive 95/46/CE and the Proposed General Data Protection Regulation".

Jiménez-Blanco, A., (1989), *"Derecho Público del Mercado de Valores"*, Ceura, Madrid.

Krause, G. y Meier, K. (edit.) (2003), "Politics, policy, and organizations: Frontiers in the scientific c study of bureaucracy", Michigan, University of Michigan Press.

Levy, B. y Spiller, P. (1996), "*Regulations, Institutions and Commitment"*, New York, Cambridge University Press.

Loewenstein, K., (1986), "*Teoría de la Constitución"*, 2º ed. Ariel, Barcelona.

López Calvo, J. (2017) *Comentarios al Reglamento Europeo de Protección de Datos*. Madrid, Sepin. Págs. 81 y siguientes.

García de Enterría, E. y Fernández, T., (2020), "*Curso de Derecho Administrativo"*, Vol. I.

Lucas Murillo, P., (1992), "El derecho a la autodeterminación informativa", Madrid.

Magide Herrero, M., (2000), *"Límites constitucionales de las Administraciones independientes,* Instituto Nacional de Administración Pública, Madrid*. (MAP-INAP)"*.

Maqueo Ramírez, M., Moreno González, J. y Recio Gayo, M., (2017), "Protección de datos personales, privacidad y vida privada: la inquietante búsqueda de un equilibrio global necesario", *Revista de Derecho*, Valdivia, vol. 30, n° 1.

Martínez López-Sáez, M., (2018), "Una revisión del derecho fundamental a la protección de datos de carácter personal", Tirant Lo Blanch, Valencia.

Matia Portilla, F. y Lopez de la Fuente, G. (2020), *"De la intimidad a la vida privada y familiar. Un derecho en construcción,* Tirant Lo Blanch, Valencia.

Mitjans Perelló, E. (2014), "Los desafíos y la experiencia de la Autoridad Catalana de protección de datos (2005-2012)", *Régimen jurídico de los derechos personales*. Abelado Perrot. Buenos Aires, Argentina.

Morales Tostado, María del Carmen, Monterde Valenzuela, María de los Ángeles, & Morales Tostado, Reyna Guadalupe. (2020). Participación de la sociedad civil en el derecho de acceso a la información pública. *Biolex, 12*(22), 79-103. Epub 28 de abril de 2021.https://doi.org/10.36796/biolex.v22i0.164

Moreno Bobadilla, A. (2017) "La influencia europea en el ámbito de los derechos fundamentales en España, en concreto en el derecho a la intimidad", *Estudios Constitucionales,* vol. 15, n°18, 1, pp. 301-330.

Moreno Bobadilla, A. (2019) "El derecho al olvido digital: una brecha entre Europa y Estados Unidos", *Revista de Comunicación* n° 18, 1, pp. 259 - 276.

Moreno Bobadilla, A. (2020) "El olvido previo a Internet: los orígenes del actual derecho al olvido digital", *Cuestiones Constitucionales.*

Moreno Bobadilla, A.y Serrano Maíllo, I. (Coord.) (2021): *El derecho al a protección de datos personales en Europa y en América: diferentes visiones para una misma realidad*. Tirant lo Blanch. Valencia.

Müller, W., "Ministerialfreie Räume", en *Juristische Schulung*.

Murga Fernández, J., (2017), "La protección de datos y los motores de búsqueda en internet: cuestiones actuales y perspectivas de futuro acerca del derecho al olvido", *Revista de Derecho Civil*, vol. IV, número 4, octubre-diciembre de 2017.

Murillo de la Cueva, L. (1999), "La construcción del derecho a la autodeterminación informativa", *Revista de Estudios Políticos (Nueva época)*, n° 104, abril-junio.

Murillo de la Cueva, P. y Piñar Mañas, J. L., (2009), "*EL Derecho a la Autodeterminación Informativa"*, Madrid, Fundación Coloquio Europeo.

Nino, C., (2002), "Fundamentos de Derecho Constitucional, Análisis filosófico, jurídico y politológico de la práctica constitucional", Buenos Aires, Editorial Astrea.

Nogueira Alvalá, H., (1998), "El Derecho a la Privacidad y a la Intimidad en el Ordenamiento Jurídico Chileno", *Ius et Praxis*, vol. 4, nº 2, Universidad de Talca, Chile.

Numan, E. J. et al. (ed.) (2010), *Massificatie in het privaatrecht*

OCDE (2005) "*Designing Independent and Accountable Regulatory Authorities for High Quality Regulation, Working Party on Regulatory Management Reform*" http://www.oecd.org/regreform/regulatory-policy/35028836.pdf

Padin Vidal, A., (2019), "Protección de datos en Colombia, Perú, México y Brasil. Referencia a Estados Unidos", en *La Adaptación al nuevo marco de protección de datos tras el RGPD y la LOPDGDD"*, Coordinador José López Clavo, Wolters Kluwer.

Pardow, D., (2018), "¿Técnicos o políticos?: Radiografía del Sistema de Nombramiento de Directores de Agencias Regulatorias Independientes", *Revista Chilena de Derecho*, Vol. 45, n° 3.

Pauner, C. y Tomás, B., (2009), "Las Agencias de Protección de Datos como Administración Independiente", en *Las Administraciones Independientes*, Tirant Lo Blanch, Valencia, 2009.

Pazos Castro, R., (2015), "El mal llamado derecho al olvido en la era de Internet", *Boletín del Ministerio de Justicia*, n° 2183, año LXIX.

Pérez Luño, A. (1989), "Los derechos humanos en la sociedad informática", *Cuadernos y Debates*, Centro de Estudios Constitucionales, Madrid.

Pérez Luño, A. (2006), "*La tercera generación de derechos humanos*", Thomson-Aranzi, Madrid.

Pérez Luño, A. (2010), "*Derechos Humanos, Estado de Derecho y Constitución*", 10a Edición. Madrid, Tecnos.

Phillipe, J. y Guyon, A.-Ch., (2015), *"Data protection in France: overview"*, Practical Law Association of Corporate Council, Global Guide 2015/2016 Data Protection (Country QUA).

Piñar Mañas, J. L. (2016), "*Reglamento General de Protección de Datos, Hacia un nuevo modelo europeo de privacidad*". Reus, Madrid

Piñar Mañas José Luis, y Recio Gayo, M. (2018). "*El derecho a la protección de datos en la jurisprudencia del tribunal de justicia de la unión europea"*. Wolters Kluwer.

Puente Escobar, A., (2008), "La Agencia Española de Protección de Datos como garante del derecho fundamental a la protección de datos de carácter personal", *Azpilcueta*, n° 20.

Puente Escobar, A. (2019), "Principio y licitud del tratamiento", en Rallo Lombarte, Artemi (dir.), Tratado de Protección de Datos. Actualizando con la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos y Garantías de Derechos Digitales, Valencia, Tirant lo Blanch.

Rajevic, E. (2010), "El Consejo para la Transparencia como Agencia Independiente", en Varios Autores (edit.) *Transparencia en la Administración Pública*, Santiago, Abeledo Perrot.

Rajevic, E. (2011), "Protección de datos y transparencia en la administración pública chilena: inevitable y deseable ponderación", *VVAA Reflexiones sobre el uso y abuso de los datos personales en Chile*, Santiago, Expansiva – Ediciones, Universidad Diego Portales.

Rallo Lombarte, A., (2012), "Hacia un nuevo sistema europeo de protección de datos: las claves de la reforma", *Revista de Derecho Político (UNRD)*, n° 85 (septiembre-diciembre).

Ramiro Arenas, M. (2006), "El derecho fundamental a la protección de datos personales en Europa". Tirant lo Blanch, Vlencia, pp. 363-374.

Rebollo Delgado, L. (1998), "Derechos de la personalidad y datos personales", *Revista de Derecho Político*, n° 44, Madrid.

Rebollo Delgado, L. (2000), "*El derecho fundamental a la intimidad*", Madrid, Dykinson.

Rebollo Delgado, L. y Serrano Pérez, M. (2008), "*Introducción a la protección de datos*", Madrid, Dykinson.

Rebollo Delgado, L. y Saltor, C. E. (2013*). "El derecho a la protección de datos en españa y argentina : orígenes y regulación vigente*". Dykinson.

Rebollo Delgado, L. (2018), "*Protección de Datos en Europa. Origen, Evolución y regulación actual"*, Madrid, Dykinson.

Reusser, C., (2018), "Derecho al olvido. La protección de datos personales como limite a las libertades informativas", Santiago, Ediciones DER.

Revenga Sánchez, M., (2014), "El Derecho a la Intimidad: un derecho en demolición (y necesitado de reconstrucción)", *Cuadernos y Debates* n° 248: El derecho a la privacidad en un nuevo entorno tecnológico, Madrid, Centros de Estudios Políticos y Constitucionales.

Rodotá, S., (2014), "*El derecho a tener derechos*", Bolonia, Trotta, Traducción de Revuelta López, J.

Rodríguez Molina, J., (2008), "La confesión auricular. Origen y desarrollo histórico*"*, *Gazeta de Antropología*, nº 24.

Rose-Ackerman, S. (1986), "¿Reforming public bureaucracy through economic incentives?", *Journal of Law, Economics and Organization*, vol. II, n° 1.

Sagüés, N., (1997), "*Elementos de Derecho Constitucional*", tomo 2, 2da. edición actualizada, Ed. Astrea, Buenos Aires, Argentina.

Sala Arquer, J., (1985), "El Estado neutral. Contribución al estudio de las administraciones independientes", AöR, nº 91.

Salvador Martínez, M., (2002), *"Autoridades independientes"*, Ariel Derecho.

Sánchez de Diego Fernández de la Riva, M.- (2010) "El derecho de acceso a la información pública", en Cotino Hueso, Lorenzo y Valero Torrijos, Julián (Coordinadores) (2010), "Administración Electrónica". La Ley 11/2007, de 22 de junio, de "acceso electrónico de los ciudadanos a los Servicios Públicos y los retos jurídicos del e-gobierno en España", Ed. Tirant lo Blanch, Valencia.

Sánchez de Diego Fernández de la Riva, M. (2013). "Transparencia y acceso a la información pública ¿son lo mismo? Por un derecho fundamental a acceder a la información pública" en Loreto Corredoira y Lorenzo Cotino (coordinadores), *Libertad de expresión e información en Internet: amenazas y protección de los derechos personales*, Madrid, Centro de Estudios Políticos y Constitucionales.

Sánchez de Diego Fernández de la Riva, M. (2019) "Dudas sobre el derecho a la actualización de informaciones en medios digitales" en en *Otro Sí* . Colegio de Abogados de Madrid. Páginas 46-47.

Sánchez de Diego Fernández de la Riva, M. y Salvador Martínez, M. (2021) *Fundamentos de la transparencia, aspectos políticos y perspectiva internacional* Foros y Debates nº 29. Madrid. Centro de Estudios Políticos y Constitucionales.

Sánchez de Diego Fernández de la Riva, M. (2022) *El derecho de acceso a la información. Un tortuoso camino*. Colección Fragua Comunicación nº 207. Madrid. Editorial Fragua.

Sanz Salguero, F. (2017), "Grado de Equivalencia entre la Protección de los Datos Personales y el Derecho de Acceso a la Información Pública", *Revista de Derecho de la Pontificia Universidad Católica de Valparaíso*, año 48, 1° semestre.

Schmidt-Assmann, E., (1993), "La legitimación de la Administración como concepto jurídico", *Documentación Administrativa*, n° 234.

Secretary General Speech, (2016), "Convention 108: from a European reality to a global treaty: Modernising the Convention", 17 June.

Seidel, U., (1974), "*Datenbanken und Datenschutz*", Frankfurt.

Sierra Rodríguez, J. (2022). "De la participación política a la participación ciudadana. Los contornos de la participación" en Sierra Rodríguez, J., Reviriego Picón, F. y Tudela Aranda, J. (Eds.) *Escenarios de la participación ciudadana: una visión multinivel*. Fundación Manuel Giménez Abad, Zaragoza.

Solove, D. y Schwartz, P., (2018),*" Information Privacy Law"*, New York, Wolters Kluwer, 6° ed.

Stephenson, M., (2007), "Bureaucratic decision costs and endogenous agency expertise", *Journal of Law, Economics and Organization*, vol. XXIII, n° 2.

Tomás Mallén, B. (2019), "Las sinergias entre el Reglamento General de Protección de Datos de la Unión Europea y el Convenio 108 del Consejo de Europa", en García Mahamut Rosario y Tomás Mallén Beatriz (eds.) *El Reglamento General de Protección de Datos: un enfoque nacional y comparado. Especial referencia a la LO 3/2018 de Protección y garantía de los derechos digitales,* Valencia. Tirant lo Blanch.

Troncoso Reigada, A. (2003), "La protección de datos personales. Una reflexión crítica de la jurisprudencia constitucional", *Cuadernos de Derecho Público*, n° 19-20.

Troncoso Reigada, A. (2016), "Autoridades de Control Independientes", en *Reglamento General de Protección de Datos, Hacia un nuevo modelo europeo de privacidad*, director Piñar Mañas, J., Reus, Madrid.

Tur Austina, R., (2006), "Cooperación en materia de terrorismo, transferencia de datos personales", Comentario a la sentencia del Tribunal de Justicia de la Unión Europea de 30 de mayo, *Revista Europea de Derechos Fundamentales*, n° 8.

Villegas Carrasquilla, L., (2012), "Protección de datos personales en América Latina: retención y tratamiento de datos personales en el mundo de Internet", en *Hacia una Internet Libre de Censura, Propuesta de América Latina*, Facultad de Derecho, Centro de Estudios en Libertad de Expresión y Acceso a la Información, compilador Eduardo Bertoni, Buenos Aires.

Violler, P., (2017), "*El estado de la protección de datos personales en Chile*", Santiago, Derechos Digitales.

Westin, A., (1970), "*Privacy and Freedom*," Ed. Atheneum, 6ª edición, Nueva York, 1970.

Wilson, J., (1989), "Bureaucracy: What government agencies do and why they do it", New York, Basic Books.

Wolfe, C., (1986), "La transformación de la interpretación constitucional", Cívitas, Madrid.

Wood, D. y Bothe, J., (2004), "Political transaction costs and the politics of administrative design", *Journal of Politics*, vol. LXVI, n° 1.

REFERENCIAS PROPIAS

Oñate Vera, E., (2019), "Internet y la importancia de un órgano de control para la protección de datos personales", en *Revista Rumbos TS*, año XIV, nº 20, diciembre, ISSN en línea 0719-7721.

Oñate Vera, E., (2021), "El derecho a la protección de datos personales en Sudamérica y su perspectiva normativa", en Moreno Bobadilla, A. y Serrano Maíllo, I.(Coord.): *El derecho a la protección de datos personales en Europa y en América diferentes visiones para una misma realidad.* Tirant Lo Blanch, Valencia.

Oñate Vera, E., (2021), "El habeas data en la nueva Constitución", en *Ideas Centrales para la nueva Constitución.* Editor Nuñez Leiva, J. Tirant Lo Blanch, Valencia.

JURISPRUDENCIA

CIDH: Corte Interamericana de Derechos Humanos; TEDH: Tribunal Europeo de Derechos Humanos; TJUE: Tribunal de Justicia de la Unión Europea; TC ESPAÑA: Tribunal Constitucional de España.

CIDH Caso Masacres de Ituango vs. Colombia, Sentencia de Fondo, de 1 de julio de 2006.

CIDH Caso Escué Zapata vs. Colombia, Sentencia de Fondo (Reparaciones y Costas), de 4 de julio de 2007.

CIDH Caso Tristán Donoso vs. Panamá, Sentencia de Fondo (Excepción Preliminar, Fondo, Reparaciones y Costas), de 27 de enero de 2009.

CIDH, Caso Escher y Otros vs. Brasil, Sentencia de Fondo (Excepción Preliminar, Fondo, Reparaciones y Costas), de 6 de julio de 2009.

CIDH Caso Fernández Ortega vs. México, Sentencia de Fondo (Excepción Preliminar, Fondo, Reparaciones y Costas), de 30 de agosto de 2010.

CIDH Caso Rosendo Cantú y Otra vs. México, Sentencia de Fondo (Excepciones Preliminares, Fondo, Reparaciones y Costas), de 31 de agosto de 2010.

CIDH Caso Familia Barrios vs. Venezuela, Sentencia de Fondo (Reparaciones y Costas), de 24 de noviembre de 2011.

CIDH. Caso Atala Riffo y Niñas vs. Chile, Sentencia de Fondo (Reparaciones y Costas), de 24 de febrero de 2012.

CIDH, Caso Artavia Murillo y Otros ("Fecundación in vitro") vs. Costa Rica, Sentencia de Fondo (Excepciones Preliminares, Fondo, Reparaciones y Costas), de 28 de noviembre de 2012.

TEDH Tyrer v. Reino Unido, Sentencia de 25 de abril de 1978.

TEDH Klass and others v. Germany, Sentencia de 6 de septiembre de 1978.

TEDH Airey, Serie A, Sentencia de 9 de octubre de 1979.

TEDH Malone v. The United Kingdom, Sentencia de 2 de agosto de 1984.

TEDH X and Y v. Netherlands, Sentencia de 26 de marzo de 1985.

TEDH Leander v. Sweden, Sentencia de 26 de marzo de 1987.

TEDH Gaskin v. The United Kingdom, Sentencia de 7 de julio de 1989.

TEDH Kruslin v. France, Sentencia de 24 de abril de 1990.

TEDH Kokkinakis c. Grecia, Sentencias de 25 de mayo de 1993.

TEDH Z. v. Finland, Sentencia del 25 de febrero de 1997.

TEDH M. S. v. Sweden, Sentencia de 2 de agosto de 1997.

TEDH Amann v. Switzerland, Sentencia de 16 de febrero de 2000.

TEDH Rotaru v. Romania, Sentencia del 4 de mayo de 2000.

TEDH Odièvre v. France, Sentencia de 13 de febrero de 2003,

TEDH Sciacca v. Italy, Sentencia de 11 de enero de 2005.

TEDH B.B. v. France, Sentencia de 17 de diciembre de 2006.

TEDH Perry c. Letonia, Sentencia de 8 de noviembre de 2007.

TEDH Z. v. Finland, Sentencia de 17 de octubre de 2008.

TEDH S. and Marper v. United Kingdom, Sentencia de 4 de diciembre de 2008.

TEDH K.U. v. Finland, Sentencia de 2 de diciembre de 2008.

TEDH Haralambie v. Romania, Sentencia de 27 de octubre de 2009.

TEDH Khelili v. France, Sentencia de 18 de octubre de 2011.

TEDH Axel Springer AG v. Germany, Sentencia de 7 de febrero de 2012.

TEDH Von Hannover v. Germany (No. 2), Sentencia de 7 de febrero de 2012.

TEDH M.K. v. France, Sentencia de 18 de abril de 2013.

TJUE de 6 de noviembre de 2003, Lindqvist, C 101/01.

TJUE de 16 de diciembre de 2008, Satakunnan Markkinapörssi y Satamedia, C 73/07.

TJUE de 7 de mayo de 2009, Rijkeboer, C 553/07.

TJUE de 9 de marzo de 2010, Comisión/Alemania, C 518/07.

TJUE de 9 de noviembre de 2010, Volker und Markus Schecke y Eifert, C 92/09.

TJUE de 16 de octubre de 2012, Comisión/Austria, C-614/10.

TJUE de 7 de noviembre de 2013, IPI, C 473/12.

TJUE de 8 de abril de 2014, Comisión/Hungría, C 288712.

TJUE de 13 de mayo de 2014, Google Spain y Google, C 131/12.

TJUE de 11 de diciembre de 2014, Ryneš, C 212/13.

TJUE de 1 de octubre de 2015, Bara y otros, C 201/14.

TJUE de 1 de octubre de 2015, Weltimmo, C 230/14.

TJUE de 6 de octubre de 2015, Schrems, C 362/14.

TJUE de 19 de octubre de 2016, Breyer, C 582/14.

TJUE de 4 de mayo de 2017, Rīgas satiksme, C 13/16.

TJUE de 27 de septiembre de 2017, Puškár, C 73/16.

TJUE de 29 de mayo de 2018, Liga van Moskeeën en Islamitische Organisaties Provincie Antwerpen y otros, C 426/16.

TJUE de 5 de junio de 2018, Wirtschaftsakademie Schleswig Holstein, C 210/16.

TJUE de 10 de julio de 2018, Jehovan todistajat, C 25/17.

TJUE de 29 de julio de 2019, Fashion ID GmbH & Co. KG contra Verbraucherzentrale NRW EV, C-40/17.

TJUE de 24 de septiembre de 2019, GC y otros contra Commission nationale de l'informatique et des libertés (CNIL), C136/17.

TJUE de noviembre de 2019, Associated Newspapers Ltd, C 687/18.

TC ESPAÑA Sentencias 254/1993 de 20 de julio.

TC ESPAÑA 292/2000 de 30 de noviembre.

TC ESPAÑA 58/2018 de 4 de junio de 2018.