

UNIVERSIDAD COMPLUTENSE DE MADRID
FACULTAD DE DERECHO
Departamento de Derecho Constitucional



**EL DERECHO FUNDAMENTAL A LA PROTECCIÓN
DE DATOS PERSONALES EN MÉXICO : ANÁLISIS
DESDE LA INFLUENCIA DEL ORDENAMIENTO
JURÍDICO ESPAÑOL**

**MEMORIA PARA OPTAR AL GRADO DE DOCTOR
PRESENTADA POR**

María de los Angeles Guzmán García

Bajo la dirección del doctor

Ildefonso Soriano López

MADRID, 2013

Tesis doctoral:

El derecho fundamental a la protección de datos personales en México.

**Análisis desde la influencia del ordenamiento
jurídico español**

María de los Angeles Guzmán García

Tutor:

Dr. Idefonso Soriano López.

Programa doctoral:

Estudios Superiores de Derecho Constitucional.
Además, con “mención de doctor europeo”.

Departamento:

Derecho Constitucional.

Universidad:

Universidad Complutense de Madrid.

Fecha:

10 de Marzo de 2013

*A mis padres,
Juan Guzmán y Mary García.*

Agradecimientos

A mis padres,

Por la invaluable paciencia y apoyo que siempre me han brindado, para ustedes mi amor, admiración y respeto siempre. A toda mi familia por su apoyo, especialmente a Nano, por el cariño y presencia diaria en estos años, y por su dedicación para demostrarme que la distancia no es un obstáculo para mantenernos cerca.

A Miguel Chávez,

Por su ayuda y apoyo que impulsaron la culminación de este proyecto, lo que ha significado un gran incentivo y motivación.

Al Profesor Ildefonso Soriano,

Por la paciencia desde el inicio en la elaboración de la tesis, así como por el apoyo a los diversos proyectos que surgieron durante esta etapa.

A mis amigos,

Especialmente a Rafa, por su cariño y apoyo en gran parte de este camino académico en Madrid. Así como a Rubén, Vanessa y Ana por su amistad.

Al Tribunal Constitucional de España,

Que gracias a su personal de doctrina e informática se convirtió inmediatamente en mi segunda casa y escuela, contribuyendo de una forma inmensurable y definitiva en mi formación profesional, académica y personal.

A las Instituciones que hicieron posible materializar este proyecto,

A mi *alma matter*, la Universidad Autónoma de Nuevo León, por el apoyo brindado al inicio de este proyecto. A la Universidad Complutense de Madrid, por ser hoy mi *alma matter* española. A la Universidad Nacional de Educación a Distancia, por formar parte importante del comienzo de este propósito. Al Centro de Estudios Políticos y Constitucionales y a su personal, no solo por la formación ahí recibida y los años que pasé en su biblioteca, sino también por haberme hecho sentir en casa este tiempo. A la Comunidad de

Madrid, a través del Instituto Madrileño del menor y la familia, por su apoyo para la realización de mi plan académico.

A España y su gente,

Por haberme hecho sentir en casa, por las oportunidades académicas y por haberme permitido realizar muchísimos proyectos. Por ello, hoy mi orgullo es doble: por ser mexicana y por los lazos culturales vinculados a España, hoy y voluntariamente adoptada, sentimentalmente, como mi segunda patria.

Índice

AGRADECIMIENTOS	3
ÍNDICE	7
SÍNTESIS.....	11
RESUMEN	19
SUMMARY.....	29
GLOSARIO	37
0. INTRODUCCIÓN	41
0. INTRODUZIONE.....	47
I. ORIGEN Y EVOLUCIÓN DEL DERECHO A LA PROTECCION DE DATOS PERSONALES	53
1. DERECHOS HUMANOS Y DERECHOS FUNDAMENTALES.....	54
2. GENERACIONES HISTÓRICAS DE DERECHOS HUMANOS	56
2.1 Generalidades de la primera y segunda generación: especial referencia a la privacidad como derecho de primera generación.	57
2.2 Derechos de tercera generación: mención a la protección de datos personales.	60
2.3 Consideración a la cuarta generación.....	62
3. DERECHOS DE LA PERSONALIDAD.....	63
4. REGULACIÓN NORMATIVA INTERNACIONAL DE LA VIDA PRIVADA	68
4.1 Declaración Universal de los Derechos Humanos.	69
4.2 Carta Internacional de los Derechos Humanos: referencia al Pacto Internacional sobre Derechos Civiles y Políticos.....	81
4.3 Declaración Americana de los Derechos y Deberes del Hombre.....	87
4.4 Convención Americana sobre Derechos Humanos.....	91
4.5 Convenio Europeo de Derechos Humanos	93
4.6 Convenio No. 108 para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal.	100
4.7 Directiva de 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.	102
4.8 Carta de los Derechos Fundamentales de la Unión Europea	104
II. EL DERECHO A LA PROTECCION DE DATOS PERSONALES Y SUS PRIMERAS INSERCIONES CONSTITUCIONALES	111
1. GENERALIDADES DE LA PROTECCIÓN DE DATOS PERSONALES.....	111
2. DEFINICIÓN FORMAL.....	114
3. DERECHO AUTÓNOMO O DERECHO DERIVADO.....	117
4. EL ORIGEN DE LA PROTECCIÓN DE DATOS PERSONALES. PRIVACIDAD Y/O INTIMIDAD.....	120
5. BIEN JURÍDICO PROTEGIDO.....	124
6. HABEAS DATA	125
7. INTIMIDAD.....	126
8. DERECHO A LA INFORMACIÓN	127
9. INSERCIONES CONSTITUCIONALES DE RELEVANCIA	131
9.1 Portugal.....	131
9.2 Alemania	135
9.3 Francia	140
9.4 España.....	142
III. PROTECCION DE DATOS PERSONALES EN ESPAÑA	145
1. LA CONSTITUCIÓN DE ESPAÑA Y EL CONTENIDO DEL ARTÍCULO 18.....	145
1.1 Derecho al honor, a la intimidad personal y familiar y a la propia imagen	147
1.2 Inviolabilidad del domicilio.....	157
1.3 Secreto de las comunicaciones.....	160

1.4 Límite al uso de la informática para garantizar el honor y la intimidad personal y familiar.....	162
2. EVOLUCIÓN DE LA JURISPRUDENCIA DEL TRIBUNAL CONSTITUCIONAL EN LA CONFIGURACIÓN DEL DERECHO A LA PROTECCIÓN DE DATOS.....	162
2.1 STC 110/1984.....	163
2.2 STC 142/1993.....	164
2.3 STC 254/1993.....	165
2.4 STC 144/1999.....	167
2.5 STC 290/2000.....	168
2.6 STC 292/2000.....	170
3. DERECHO DE PROTECCIÓN DE DATOS PERSONALES	174
3.1 Objetivo	175
3.2 Función	176
3.3 Titulares.....	177
3.4 Contenido.....	178
3.5 Tipo de datos	180
3.6 Derechos de las personas	182
3.6.1 Derecho a impugnación de valoraciones.....	183
3.6.2 Derecho de consulta	186
3.6.3 Derecho de acceso.....	187
3.6.4 Derecho de rectificación y cancelación	189
3.6.5 Derecho de oposición	196
3.6.6 Derecho de indemnización	199
3.6.7 Tutela de los derechos (reclamación y la tutela de los derechos)	201
3.7 Límites.....	202
4. PRINCIPIOS EN EL TRATAMIENTO	206
4.1 Calidad de los datos.....	208
4.2 Información previa.....	211
4.3 Consentimiento.....	213
4.4 Atención a datos especialmente protegidos.....	215
4.5 Seguridad.....	218
4.6 Deber de secreto.....	220
4.7 Comunicación de los datos (cesión).....	221
4.8 Acceso a los datos por cuenta de terceros.....	223
5. NORMAS REGULADORAS DEL TRATAMIENTO DE DATOS PERSONALES EN ESPAÑA.....	224
IV. PROTECCION DE DATOS PERSONALES EN MEXICO	229
1. ANTECEDENTES	229
3. DEFINICIÓN	231
3. SUJETOS	233
4. OBJETO	234
5. LÍMITES	236
6. AUTORIDADES.....	245
6.1 El Instituto Federal de Acceso a la Información y Protección de datos personales	246
6.2 Autoridades reguladoras	247
7. PRINCIPIOS DE LA PROTECCIÓN DE DATOS PERSONALES EN POSESIÓN DEL SECTOR PÚBLICO	251
7.1 Licitud	252
7.2 Calidad de los datos.....	252
7.2.1 Acceso y corrección	253
7.2.2 De Información	253
7.2.3 Seguridad.....	253
7.2.4 Custodia y cuidado de la información	254
7.2.5 Consentimiento para la transmisión.....	254
8. PRINCIPIOS DE LA PROTECCIÓN DE DATOS PERSONALES EN POSESIÓN DE PARTICULARES	256
8.1 Licitud	256
8.2 Consentimiento.....	257

8.2.1 Características del consentimiento	258
8.2.2 Tipos de consentimiento	258
8.2.3 Datos financieros y patrimoniales	259
8.2.4 Datos sensibles	259
8.2.5 Excepciones al consentimiento	260
8.3 Información	262
8.3.1 Información que debe de contener el aviso de privacidad	262
8.3.2 Formato del aviso de privacidad	263
8.3.3 Datos obtenidos indirectamente del titular y datos con fines históricos, estadísticos o científicos.	265
8.4 Calidad	265
8.5 Finalidad	266
8.6 Lealtad	266
8.7 Proporcionalidad	267
8.8 Responsabilidad	267
8.8.1 Seguridad	269
8.8.2 Deber de secreto	269
8.8.3 Delitos en materia de tratamiento indebido de datos personales	270
9. DERECHOS DE LOS TITULARES DE DATOS PERSONALES	270
9.1 Acceso	271
9.2 Rectificación	272
9.3 Cancelación	272
9.4 Oposición	273
9.5 Procedimiento de solicitud de los derechos ARCO	274
9.5.1 Solicitud	275
9.5.2 Negativa de solicitud	276
9.5.3 Costo legal	277
10. NORMATIVIDAD APLICABLE	277
10.1 Constitución Política de los Estados Unidos Mexicanos	279
10.2 Ley Federal de Protección de Datos Personales en Posesión de los Particulares	282
10.3 Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares	284
10.4 Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental	287
10.5 Reglamento de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental	287
10.6 Lineamientos de Protección de Datos Personales	288
11. CRITERIO DE LA SUPREMA CORTE DE JUSTICIA DE LA NACIÓN SOBRE LA VIDA PRIVADA.	288
12. CRITERIO DE LA SUPREMA CORTE DE JUSTICIA DE LA NACIÓN SOBRE EL DERECHO A LA PROTECCIÓN DE DATOS PERSONALES.	290
13. TENDENCIAS	293
13.1 Internet y las redes sociales	293
13.2 Riesgos y problemas actuales en Internet	298
A. Suplantación de la identidad	298
B. Derecho al olvido	298
C. Pérdida de información	299
13.3 Niños y adolescentes	299
A. Cyberbullying	300
B. Grooming	302
C. Sexting	302
V. CONCLUSIONES	305
V. CONCLUSIONI	317
BIBLIOGRAFÍA1. MONOGRAFÍAS	329
2. INSTRUMENTOS INTERNACIONALES O REGIONALES	343
3. LEGISLACIONES NACIONALES	344
4. SENTENCIAS DEL TRIBUNAL EUROPEO DE DERECHOS HUMANOS	345

5. SENTENCIAS DEL TRIBUNAL CONSTITUCIONAL.....	347
6. AUTOS DEL TRIBUNAL CONSTITUCIONAL.....	348
7. SENTENCIAS DE LA AUDIENCIA NACIONAL.....	348
8. DICCIONARIOS Y ENCICLOPEDIAS	348
9. BOLETINES Y DIARIOS OFICIALES	348
10. OTRAS FUENTES	348
ANEXOS. RESOLUCIONES DEL IFAI DE PROTECCIÓN DE DATOS PERSONALES	351
RESOLUCIÓN 676/2005, DE 17 DE AGOSTO	351
RESOLUCIÓN 932/2005, DE 11 DE JUNIO	354
RESOLUCIÓN 1659/2005, DE 23 DE NOVIEMBRE	360
RESOLUCIÓN 187/2007, DE 25 DE ABRIL.....	366
RESOLUCIÓN 487/2007, DE 25 DE ABRIL.....	376

Síntesis

Esta tesis surge de la idea de analizar el nuevo derecho a la protección de datos personales, nacido en Europa y proyectado en las últimas décadas en Latinoamérica. Este trabajo se centra particularmente en el caso mexicano, que desde el año 2001 hubo de ver frustrados los intentos de implementar este derecho en iniciativas que no dieron fruto alguno. La Constitución mexicana, lentamente, se ha reformado en esta materia. Estos cambios a la Carta Magna inician en 2002 al mencionar en el art. 6 el derecho a la protección de datos personales en relación con el derecho a la información. Posteriormente, en 2009 las reformas constitucionales de los arts. 16 y 73, en las que se establece este nuevo derecho en el apartado sobre garantías individuales y se otorgan facultades al Congreso para legislar en este ámbito.

Después, en el año 2010 surge la Ley de Protección de Datos Personales en Posesión de los Particulares y cuyo Reglamento se publica en 2011. Este estudio también se centra en el caso español, debido a que es una fuente importante y significativa en el desarrollo de este derecho, y de su legislación en México, debido a las características culturales que comparten, producto de los vínculos históricos. Por ello, se verá que la legislación fue influenciada por la experiencia española en lo que hace a su contenido y en la proyección hacia los nuevos retos que se presentan como consecuencia del desarrollo tecnológico actual.

El primer capítulo se refiere al origen y evolución del derecho a la protección de datos personales a partir del derecho a la privacidad, este último reconocido en los distintos instrumentos internacionales del siglo XX. El segundo apartado corresponde a desarrollar distintos conceptos en torno a este nuevo derecho, así como a revisar sus inserciones constitucionales en los principales países europeos que han contribuido a su promoción constitucional como derecho fundamental. La sección tercera, atañe al desarrollo jurisprudencial y legislativo de este derecho en España. Finalmente, el último título se dedica al derecho fundamental a la protección de datos personales en México, los criterios de la

Suprema Corte de Justicia mexicana al respecto, su estructura constitucional y la legislación emitida recientemente.

Palabras Clave: derechos humanos, derechos fundamentales, Constitución, Derecho Constitucional, protección de datos personales, *habeas data*, privacidad, intimidad, jurisprudencia, *Internet*, Tribunal Constitucional, Suprema Corte de Justicia de la Nación, Tribunal Europeo de Derechos Humanos, España, México.

Abstract

This thesis is based on the analysis of the right of personal data protection, which started in Europe and has expanded throughout Latin America in recent years. This research paper focuses particularly on the Mexican case dating from 2001 when initiatives to implement this right translated into fruitless efforts. The Mexican constitution was slowly reformed, first in 2002 with article no. 6 regarding personal data protection related to the rights to information. Later, in 2009 constitutional reforms to articles no. 16 and 73 were made to establish this new right as part of the individual rights, and giving the congress the power to legislate in this matter.

In 2010, the Personal Data Protection Law held by Private Entities was passed and the subsequent regulation was published in 2011. This study also discusses the Spanish case, which acts as an important and relevant source in the development of this right and its legislation in Mexico due to the cultural characteristics shared by both countries, a result of their historical ties. In this context, it's evident that the legislation was influenced by the Spanish experience regarding its contents and its projection towards the new challenges that derive from technological development.

The first chapter deals with the origin and evolution of the right to personal data protection as a right to privacy, which was internationally recognized in several laws in the 20th century. The second chapter is devoted to the development of different concepts regarding this new right, as well as the review of constitutional reforms in the main European countries that have contributed to its promotion as a fundamental right. The third chapter gives an account of the jurisprudential and legislative evolution of this right in Spain. Finally, the last chapter presents the fundamental right to data protection in Mexico, the criteria of the Mexican Supreme Court of Justice regarding this issue, its constitutional structure and the recent approved laws in this area.

Keywords: human rights, fundamental rights, Constitution, Constitutional Law, personal data protection, protection of personal data, *habeas data*, privacy,

private life, jurisprudence, Internet, Constitutional Court, Supreme Court of Justice of the Mexican Nation, European Court of Human Rights, Spain, Mexico.

Abstrait

Cette thèse découle de l'idée d'analyser droit à la protection des données personnelles, né en Europe et développé dans les dernières décennies en Amérique latine. Ce travail se concentre particulièrement sur le cas du Mexique, qui depuis 2001 a souffert des tentatives frustrées de mettre en œuvre ce droit dans des initiatives qui n'ont pas portées de fruits. La Constitution mexicaine a pâti des réformes à pas lent: d'abord en 2002, ce qui est mentionné dans l'article 6, le droit à la protection des données personnelles en relation avec le droit à l'information. Plus tard, en 2009, les réformes constitutionnelles des articles 16 et 73, dans l'établissement de ce nouveau droit dans la section des garanties individuelles, et qui autorise le Congrès à légiférer dans ce domaine.

La loi sur la protection des données personnelles détenues par les particulières émerge à 2010, tandis que son règlement est publié en 2011. Cette étude se concentre également sur le cas espagnol, car il est une source importante et significative dans le développement de ce droit et de la législation au Mexique en raison des caractéristiques culturelles qu'ils partagent, en raison de liens historiques. Ainsi, nous voyons que la loi a été influencée par l'expérience espagnole en ce qui concerne leur contenu et la projection des nouveaux défis posés produit du progrès technologique.

Le premier chapitre correspond à l'origine et l'évolution du droit à la protection des données personnelles à partir du droit à la confidentialité, celui-ci reconnu dans les instruments internationaux du XXème siècle. Le deuxième chapitre se rapporte à développer des concepts différents sur le droit à la protection des données personnelles et de l'examen de ces nouveautés dans le droit constitutionnel dans les principaux pays européens qui ont contribué à sa promotion en tant que droit fondamental. Le troisième chapitre se réfère au développement de cette jurisprudence et le droit législatif en Espagne. Enfin, le dernier chapitre est consacré au droit fondamental à la protection des données personnelles au Mexique, les critères de la Cour suprême mexicaine à cet égard, sa structure constitutionnelle et les lois adoptées récemment.

Mots-Clés: droits de l'homme, droits fondamentaux, Constitution, Droit Constitutionnel, protection des données personnelles, *habeas data*, privacité, vie privée, intimité, jurisprudence, *Internet*, Tribunal Constitutionnel, Cour Suprême de Justice de la Nation, Cour Européenne des droits de l'Homme, Espagne, Mexique.

Riassunto

Questa tesi nasce dalla idea di analizzare il diritto alla protezione dei dati personali nato in Europa e proiettato, negli ultimi decenni in America Latina. Questo lavoro si concentra particolarmente sul caso messicano il quale, a partire dal 2001 ha visto del tutto frustrati gli intenti di implementazione di questo diritto, nell'ambito di iniziative che non diedero mai alcun frutto. La Costituzione messicana è stata interessata da riforme in tempi molto lenti: con la prima, nel 2002, si introdusse nell'art. 6 il diritto alla protezione dei dati personali in relazione al diritto alla informazione. Successivamente, nel 2009 si ebbero le riforme costituzionali degli Artt. 16 e 73, con le quali si sancì tale nuovo diritto nell'ambito delle garanzie individuali e, nello stesso tempo, si conferì al Congresso potestà legislativa in materia.

Nel 2010 fu varata la legge di protezione dei dati personali in possesso dei privati il cui regolamento fu pubblicato nel 2011. Questo studio, si concentra anche nel caso spagnolo, dal momento che è una fonte importantissima e significativa per lo sviluppo di questa normativa in messico, date le caratteristiche culturali condivise, in forza dei vincoli storici tra i due paesi. Per questa ragione, si vedrà come la legislazione messicana è stata influenzata dall'esperienza spagnola per ciò che concerne il suo contenuto e alla proiezione verso le nuove istanze dell'attuale progresso tecnologico.

Nel primo capitolo verranno trattati l'origine e l'evoluzione del diritto al trattamento dei dati personali a partire dal diritto alla riservatezza, quest'ultimo riconosciuto nei diversi strumenti di diritto internazionale del XX secolo. Nel secondo, invece, si porterà a compimento uno studio circa lo sviluppo di diversi aspetti afferenti al diritto alla protezione dei dati personali e delle distinte esperienze avutesi, in merito, nei principali ordinamenti giuridici europei che hanno contribuito alla costituzionalizzazione di questo diritto, come diritto fondamentale. Il terzo capitolo tratterà dello sviluppo giurisprudenziale e legislativo di questo diritto in Spagna. Al termine, l'ultimo capitolo sarà dedicato al diritto alla protezione dei dati personali in Messico, i criteri elaborati ed

utilizzati dalla Suprema Corte di Giustizia messicana, nonché la struttura costituzionale e la legislazione recentemente approvata.

Parole chiave: diritti umani, diritti fondamentali, Costituzione, Diritti Costituzionale, protección de datos personales, *hábeas data*, privacy, vita privata, intimità, giurisprudenza, *Internet*, Corte Costituzionale, Corte Suprema di Giustizia della Nazione, Corte Europea dei diritti dell'uomo, Espagne, Messico.

Resumen

a) Introducción

Esta investigación aborda el tema del derecho fundamental a la protección de datos personales en México, desde el análisis de la influencia que ha tenido el ordenamiento jurídico español, en la actual implementación normativa de este derecho en el Estado mexicano. Esta tesis se ha enfocado en analizar las principales características y diferencias que este hubo de adoptar para el caso español y mexicano. En este sentido, el trabajo destaca los principales elementos de carácter histórico que han determinado la configuración de este derecho hasta nuestros días.

El derecho a la protección de datos personales es un claro producto de la época actual en torno a la evolución de las nuevas tecnologías. En las últimas tres décadas, el tema ha tenido una rápida evolución, principalmente por el uso de Internet y los riesgos que implica. Este derecho garantiza a la persona un poder de control y disposición sobre sus datos personales, permitiéndole consentir su recogida y uso, así como a saber quién los posee y con qué finalidad.

Tanto en México como en América Latina, España ha sido un país de gran influencia debido a los fuertes lazos de cooperación forjados a lo largo de la historia. En consecuencia, el ámbito jurídico no ha sido la excepción. Por tanto, no es de extrañar, que a partir de la LORTAD y de la actual LOPD, el desarrollo de la normatividad referente al derecho de protección de datos personales haya evolucionado, repercutiendo en el surgimiento de legislaciones similares en países como Argentina, Colombia, Costa Rica, Perú y México.

Así, intentaré presentar una perspectiva global de este nuevo derecho fundamental en México, analizando su origen europeo y la necesidad de la realidad actual que ha llevado al país a la importación de este nuevo derecho fundamental, así como los mecanismos de garantía instituidos por la Ley de la materia. De igual manera, se analizarán algunos de los retos que la regulación normativa presenta, y no solo por su reciente configuración, sino porque la misma

no resuelve los problemas propios que emergen de la realidad actual en la que la sociedad se desarrolla.

b) Herramientas académicas aprovechadas.

Para la elaboración de esta tesis, además de los cursos de doctorado y de las fuentes bibliográficas consultadas, realicé múltiples seminarios, entre los que destacan aquellos sobre derechos fundamentales, protección de datos personales, Derecho Constitucional y Derecho Internacional Público. Todos ellos, de utilidad para mantenerme actualizada en lo que hace a los problemas y tendencias actuales de nuestro campo de investigación.

Asimismo, tuve la ocasión de realizar dos estancias cortas de investigación en Francia. La primera, en el “Instituto Internacional de Derechos Humanos, Rene Cassin” en Estrasburgo, donde asistí a diversos cursos de gran utilidad para profundizar en el conocimiento de los distintos sistemas de protección de derechos humanos, así como de los mecanismos para su defensa y garantía, lo que fue conveniente para la elaboración de la primera parte de esta investigación. La segunda, en la Universidad Sorbona de Paris, donde llevé a cabo cursos de Derecho Civil francés y de Derecho Internacional Privado, que fueron enriquecedores para tener una comprensión global de los derechos personales, que para este trabajo hubo de ser de utilidad en el análisis de las tendencias actuales de Derecho, principalmente, las relativas a la intimidad.

Posteriormente, tuve la invaluable oportunidad de que el Tribunal Constitucional español, me formara como Analista de Doctrina Constitucional, formación que ha contribuido en mi comprensión del sistema jurídico español, principalmente, en el campo de la de Justicia Constitucional. Las habilidades aquí adquiridas, fueron de gran ayuda para el análisis de la jurisprudencia constitucional utilizada en el apartado de la construcción jurisprudencial del derecho fundamental a la protección de datos personales en España, así como en el análisis de los ordenamientos jurídicos.

Adicionalmente, y para optar a la “Mención de Doctor Europeo”, realice una estancia de investigación en Italia, durante la cual desarrolle parte de este

trabajo en diversos centros de la Universidad de Bolonia, tales como: el Departamento de Ciencia Jurídica “Antonio Cicu”, el Centro de Estudios Constitucionales y Desarrollo Democrático, y el Spisa (Escuela de Especialización en Ciencia Administrativa). Durante este periodo hube de profundizar en la técnica de la elaboración de estudios jurídicos mediante el Derecho Comparado, herramienta que me fue de gran utilidad en el análisis del derecho a la protección de datos personales en distintos ordenamientos jurídicos.

Por último, y en cuanto a la formación jurídica recibida, también contribuyeron enormemente, para la redacción de esta tesis, los conocimientos adquiridos en las materias del programa del Máster en Derecho Constitucional y Ciencia Política que imparte el Centro de Estudios Políticos y Constitucionales; así como las asignaturas del Máster en Diplomacia y Relaciones Internacionales impartido por la Escuela Diplomática.

c) Metodología utilizada.

Para la elaboración de la presente investigación se ha utilizado el método analítico-comparativo del derecho a la protección de datos personales, para proporcionar una perspectiva del estado actual de este derecho fundamental en México. Así, Este trabajo se ha elaborado a partir del estudio del derecho español, observando los avances legislativos que México ha tenido durante los últimos años, que a partir de 2009, han sido bastantes significativos dadas las reformas constitucionales acaecidas. Afortunadamente y desde 2010, México cuenta con una Ley Federal de Protección de Datos Personales en posesión de particulares.

Sin embargo, este notable retraso en la emisión de la Ley vuelve al país vulnerable ante la protección y garantía de este derecho. Lo anterior, no solo es así por lo que implica el arduo proceso de implementación de una ley, sino porque además ha de lidiar con los avatares propios de los vertiginosos avances de la tecnología y la transmisión de la información, a la que se enfrentan países avanzados en este tema, como es el caso de España.

La presente investigación se estructuró en función de cuatro apartados, todos importantes para una adecuada comprensión del tema, iniciando por las

generalidades del origen del derecho a la protección de datos personales, continuando con las primeras inserciones constitucionales en el mundo de este nuevo derecho, después abordando el tema sobre el caso español que ha sido el principal referente en México y concluyendo con la situación actual del Estado mexicano y de su reciente legislación en este ámbito.

d) Conclusiones y resultados alcanzados.

En la última parte de este trabajo se recogen algunas consideraciones finales, que hacen énfasis a los retos que habrá de enfrentar la Ley Federal de Protección de Datos Personales, para lograr una rápida y adecuada evolución, que sitúe a México en un nivel de garantía similar al de las naciones más adelantadas en la materia. En este sentido, se destaca la autonomía que al día de hoy ha alcanzado el derecho a la protección de datos personales en cuanto a su definición; y la delimitación que ha proporcionado, respecto del derecho a la intimidad, la jurisprudencia del Tribunal Constitucional de España, la cual ha sido de gran utilidad en las recientes legislaciones iberoamericanas.

Asimismo existe la necesidad de estandarizar la normativa en la materia a nivel internacional, ya que hoy en día, debido a la instantaneidad y ubicuidad de la sociedad en la era de la globalización, el comportamiento de los individuos ha tendido a homogenizarse culturalmente. Por ello, la solución a las necesidades y la expansión de los problemas que las nuevas tecnologías han traído consigo son muy similares en cualquier parte del globo.

Por su parte, este derecho también puede presentar colisión con otros derechos fundamentales como la dignidad, privacidad, propia imagen, honor, vida, información. Lo que habrá de resolverse atendiendo a cada caso y recurriendo a la técnica de la ponderación de derechos. Sin embargo, es de precisar que en la actividad de los órganos de la Administración Pública, habrá de primar la máxima transparencia debido al origen de sus ingresos a partir de los impuestos gravados al ciudadano, salvo por las restricciones que la ley precise. En México, se ha avanzado desde hace años en la publicidad de la remuneración de los servidores públicos porque provienen de la contribución ciudadana, y sería un retroceso que a partir de la introducción de este derecho en México se llegará

a sostener en algún momento, que dicha información es un dato personal de carácter patrimonial y por ende no susceptible de revelar.

Actualmente, la sociedad se encuentra en un cambio estructural que transcurre en la era de la globalización y las nuevas tecnologías, que relaciona a todos los individuos entre sí, en función de diversos roles. Por ello, la información que fluye en dichas interacciones debe preservar derechos de la persona como la privacidad y la protección de datos personales.

En este sentido, y como se deduce del análisis de los sistemas jurídicos español y mexicano, en materia de protección de datos, no ha sido una constante comparación en paralelo, dado que el surgimiento del derecho no se presenta en una misma línea temporal. México, respecto de España, presenta un desfase de casi dos décadas, contadas desde la publicación de la primera normativa española de protección de datos personales de 1992 (LORTAD) –la posterior y actualmente vigente es la LOPD de 1999- hasta la Ley mexicana de 2010. Esta situación convierte al país en vulnerable, ya que el estado mexicano está en un proceso de implementación y adecuación de la normativa, así como de concientización de la población. La vulnerabilidad también se presenta en cuanto a la ausencia de una adecuada delimitación judicial y jurisprudencial del derecho, lo que no es de extrañar dada su reciente incorporación al ordenamiento jurídico.

El derecho a la protección de datos personales en México aparece por primera vez en el año 2002 en la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental. Después, con las reformas constitucionales de 2009, de los artículos 16 y 73. Evolución legislativa que concluye, recientemente, con la publicación de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (2010), y de su Reglamento (2011). Este primer surgimiento fue poco eficaz, ya que entonces, solamente se refería en la Ley de Transparencia la protección de datos personales en posesión de la administración pública y no aquellos en posesión de particulares, como ocurre actualmente.

Dicho sea de paso, que además esta escueta regulación del derecho a la protección de datos se asoma en el 2002, año en que aparece en México la Ley de

Transparencia. Así entonces, y dada la historia del país en temas de corrupción, el esfuerzo se condujo hacia el objeto principal de dicha Ley, es decir, la transparencia y el acceso a la información pública. Por ende, no se desarrolló adecuadamente el derecho a la protección de datos personales. Hoy en día, el derecho a la transparencia se encuentra en una etapa de madurez, y las necesidades de la sociedad actual requieren además de la consolidación del derecho a la protección de datos personales, a fin de tener el poder de disposición de su propia información.

Producto de los vínculos históricos y de cooperación con España, de la lectura de la Ley mexicana, se desprende la marcada influencia que ha tenido la experiencia española y los principales temas de discusión en la actualidad entre los especialistas, derivados de la realidad tecnológica del momento, por ejemplo el *cloud computing* en el art. 52 RLOPD, que es una nueva forma de almacenar información y cuya regulación no es fácil, por no haber una legislación internacional estándar. Así como, la aclaración del derecho de oposición en la Ley (arts. 8 y 27 LPDP), omisión que en Ley española ha dado lugar a alguna crítica (arts. 34 a 36 RLOPD), y que en la mexicana es una clara rectificación.

Hoy México reconoce la importancia del derecho fundamental a la protección de datos personales. Aunque tardíamente cuenta con una Ley especializada y su Reglamento. Por lo tanto, es urgente la actuación de los titulares del derecho en la exigencia del respeto al mismo. Sin embargo, el ejercicio de este derecho brillará por su ausencia, en tanto en cuanto, la persona no tenga conocimiento de los derechos y acciones que le asisten.

Los principios que los responsables deberán observar, cumplen con la finalidad de la necesidad actual y son acordes a los requerimientos internacionales. Sin embargo, y dado que se cuenta con una regulación diferenciada de los datos en posesión del sector público y el privado, es conveniente una adecuada unificación, a fin de que la normativa de este nuevo derecho sea más clara para el usuario. En el caso del sector público, los principios se encuentran en Lineamientos y no en un Reglamento, como es el caso del sector privado.

En lo que hace al principio de consentimiento, se establecen dos tipos: el expreso y el tácito. Este último, a diferencia de otros países, es una novedad mexicana, y consiste en aquel que se otorga cuando habiéndose puesto a su disposición el aviso de privacidad, el titular no manifiesta su oposición. El consentimiento tácito será válido como regla general, salvo que la Ley exija el consentimiento expreso (arts. 13 y 14 RLPDP). Ahora bien, y debido a la reciente innovación de esta tipología, el reglamento no es claro en el mecanismo que se habrá de seguir en el propio aviso de privacidad, para que el titular manifieste su negativa al tratamiento.

De igual modo, que existen certificaciones internacionales en este ámbito, es importante crear un mecanismo similar de validez a nivel nacional, regulado por el Instituto y cuya licencia se otorgue a profesionales técnico-especializados en la materia. Lo anterior, conducirá a paso firme hacia la urgente homogenización de procesos en protección de datos. En consecuencia, se promovería el interés de la comunidad jurídica en esta área para lograr avances significativos en el cumplimiento de la LPDP, además se incentivaría la cooperación y participación internacional en este campo.

La Ley mexicana, comparada con la española, no contempla el registro de Ficheros ante la Autoridad reguladora, lo que puede representar riesgos para el individuo por parte del Responsable o encargado. Si quien recopila la información no tiene clara la Ley, ni los datos que puede tratar –lo que no es raro cuando se está en fase de implementación de una nueva normativa-, existe el peligro de crear ficheros y tratar información excesiva por no estar correctamente asesorados. La inscripción de ficheros es una medida que, en este caso, podría ser preventiva para no almacenar datos personales en una base de datos sensibles, que con posterioridad resultase ilegal.

La normativa mexicana no prevé la implementación de diferentes grados de seguridad dependiendo del tipo de datos personales a tratar. Las medidas previstas por el Reglamento pueden dar lugar a dudas, para lo cual sería importante un instrumento especial que regule distintos niveles de seguridad a cumplir por el Responsable y el encargado.

La presencia de una persona delegada para el cumplimiento de la normativa de protección de datos en cada empresa o institución, es importante para una adecuada implementación de la Ley. Esta práctica, además incentivaría la creación de empleo y especialización de profesionales en la materia.

El tabulador de sanciones en el caso mexicano (arts. 64 a 66 LPDP), es más elevado que el español, aunque con la significativa mención de la Ley en atender a la “capacidad económica del responsable”, lo que habrá de determinarse por la autoridad competente. Por otro lado, se encuentran tipificados en la propia Ley de protección de datos, los delitos en materia de tratamiento indebido de datos personales. Ambas situaciones, constituyen por si solas un incentivo para el cumplimiento de la Ley. Sin embargo, y por ser una legislación nueva, mientras no se comience a llevar a cabo las multas y tipificaciones de delitos, la normativa no solo no se cumplirá, sino que se vulnerará deliberadamente.

Es interesante y acertada la tipificación de delitos en el capítulo XI de la Ley Federal de protección de datos personales en posesión de los particulares, sobre delitos en materia del tratamiento indebido de datos personales, que regula los actos constitutivos de delitos especiales en esta área. Esto es una novedad legislativa, por no encontrarse tipificados dentro de la propia Ley de la materia en otros países como España, Argentina, Costa Rica o Perú.

El habeas data es una garantía constitucional existente en países latinoamericanos, cuya diferencia principal radica en ser un Recurso que se promueve ante un órgano judicial, y no de un procedimiento de naturaleza administrativa, como es el caso de los países europeos. Esto responde a necesidades históricas propias de los sistemas de gobierno dictatoriales que hubo en América Latina.

Estamos de acuerdo con la garantía que proporciona un órgano administrativo especializado en la materia. Sin embargo, a la par de ello, es conveniente, principalmente para la fortificación del derecho fundamental, que se prevea el recurso de Habeas Data en México, para situaciones de máxima seguridad como por ejemplo los que tienen que ver con los datos sensibles,

seguridad y defensa de grandes colectivos, así como los que se refieren a evidentes intereses nacionales.

Finalmente, se reitera la existencia de la necesidad de que el Instituto emprenda una trascendental labor de divulgación, mediante la cual la ciudadanía conozca la existencia de este nuevo derecho y de los mecanismos para hacerlo valer. Así, el IFAI emitirá resoluciones, que eventualmente serán recurridas ante el Poder Judicial Federal y este dictará Sentencias que habrán de aclarar y configurar cada día este nuevo derecho.

Summary

a) Introduction

The subject of this research is the case of the fundamental right of personal data protection in Mexico. It stems from the analysis of the influence of the Spanish legal framework over the law implementation of this right in Mexico. This dissertation focuses on the main characteristics and differences between the Spanish and the Mexican cases, identifying the main historic elements which determined the configuration of this right, until today.

The personal data protection right is a clear product of the development of the new technologies typical of the current era, and it has rapidly evolved over the last three decades, mainly due to the use of the Internet and the risks this entails. This right guarantees the individual control and disposition of personal data, enabling the owner to allow its collection and use, as well as to know who possesses it and for what purpose.

Spain has historically exercised great influence upon both Mexico and Latin America, because of the tight cooperation relationship between these countries; thus, the juridical sphere makes no exception. As a consequence, it is not surprising that - since the LORTAD and the current LOPD – the advances in the personal data protection right regulations have affected the development of similar legislations in countries such as Argentina, Colombia, Costa Rica, Peru and Mexico.

This dissertation aims at providing a comprehensive view of this new fundamental right in Mexico, based on: the analysis of its European origins; the current calls for its implementation in Mexico; and the guarantee mechanisms established by the Law. Equally, attention will be drawn to some of the challenges this new regulation faces, not only due to its recent configuration, but also because it fails to solve the problems typical of the current social framework.

b) Academic tools

For the purpose of this dissertation – besides the doctoral courses I have attended and the bibliographic sources I have drawn upon – I have attended several seminars focused on fundamental rights, personal data protection, Constitutional Law, and International Public Law, among others. This was of great use for keeping abreast of the current issues and trends related to the research.

In addition, I had the opportunity to carry out two short research stays in France. During the first one - at the “International institute of Human Rights, Rene Cassin”, in Strasburg – I attended several courses which were extremely useful to delve into the various systems of human rights protection, and their guarantee mechanism. This turned out to be extremely advantageous for the elaboration of the first part of this research. The second stay was at the Paris-Sorbonne University, where I attended courses of French Civil Law and International Private Law. This was enlightening for a thorough comprehension of personal rights, which was useful for the analysis of the current legal trends, especially the ones related to the concept of privacy.

Subsequently, I had the precious opportunity to be trained at the Spanish Constitutional Court as analyst of Constitutional policy. This training contributed to my comprehension of the Spanish legal system, mainly in the field of Constitutional Law. The skills I acquired there have been key tools for the analysis of the Constitutional Law, encompassed in the section addressing the legislation of the fundamental right of personal data protection in Spain, as well as for the analysis of the legal frameworks.

Additionally, in order to opt for the Mention of “European Doctor”, I carried out a research stay in Italy where I elaborated part of this work in several departments of the University of Bologna, including: the Juridical Science Department “Antonio Cicu”, the Centre of Constitutional Studies and Democratic Development, and the SPISA (Specialization School of Administrative Science). During this stay, I could enrich my research skills in legal studies thanks to the

analysis of Compared Law. This tool has been extremely useful for the analysis of the right of personal data protection within several legal frameworks.

Finally – as for my juridical training – the education derived from the course subjects of the Constitutional Law and Political Science Master’s degree, at the Centre of Political and Constitutional Studies, also contributed to the composition of this work; as well as the subjects of the Master’s degree in Diplomacy and International Relations from the Diplomatic School.

c) Methodology

A comparative analysis method of the personal data protection right has been used for the elaboration of this research, with the aim to provide a comprehensive view of the current situation of this fundamental right in Mexico. Thus, this work has developed from the analysis of the equivalent Spanish right, focusing on the legislation advances which took place in Mexico over the last years. These advances have been very significant due to the constitutional reforms enacted since 2009. Since 2010, Mexico has fortunately implemented the Federal Law for the Protection of Personal Data in possession of private individuals.

However, the late enactment of the law jeopardizes the protection and the guarantee of this right in this country. This is not only due to the hard implementation process of the law, but also to the continuous striving to cope with the dramatic advances of technology and information transmission, which are faced by countries in the forefront in this area, such as Spain.

This research is structured according to four sections, which are all equally important for the comprehension of the topic. First, the origin of the right of personal data protection is introduced; and its first constitutional insertions in the legal framework are reviewed. Subsequently, the Spanish case is examined since it has constituted the main Mexican reference; finally, focus is shifted to the current situation of the Mexican recent legislation.

d) Conclusions

The last section of the dissertation provides some final considerations, addressing the challenges to be faced by the Federal Law for Personal Data Protection for a prompt and appropriate development, in order to raise the Mexican legal guarantee to the level of the most developed countries in this matter. Therefore, as far as the right of personal data protection is concerned, it is worth mentioning: the current level of autonomy of its definition; its legal delimitation - with respect to the right of privacy – produced by the ruling of the Spanish Constitutional Court, which proved its effectiveness in the recent Latin American legislations.

Nonetheless, the legislations on the matter need international standardizing. Nowadays, this is due to the instantaneous and ubiquitous nature of our globalised society which, on a cultural level, has tended to homogenize individual behaviours. As a consequence, both the solutions to the human needs and the increasing problems brought about by the new technologies have been very similar worldwide.

On the other hand, this right can conflict with other fundamental rights including dignity, privacy, self-image, honour, life, and information rights. These rights are to be complied with by case studies solutions and the weighting of the rights involved. However, it must be pointed out that extreme transparency is needed among the Public Administration Bodies, since their income sources derive from public taxes, with exception of law-enforced restrictions. For some years now, the publicizing of civil servants' salaries has increased, for they derive from state taxes. Therefore, it will be a setback if one can ever claim – after this new right has been implemented in Mexico – that such information lies in the property-related realm of personal data, hence subject to non-disclosure restrictions.

In the era of globalization and new technologies, society is currently going through a structural change which is linking the individuals together according to several roles. Therefore, the information flowing through such

interactions has to protect individual rights, such as privacy and personal data protection.

In this sense – as the analysis of the Spanish and Mexican legal systems pinpoints – in the realm of data protection, the evolution of the two systems has not been constantly parallel, since their respective developments do not lie in the same temporal line. In comparison with Spain, Mexico has a phase difference of nearly two decades, since the 1992 publication of the first Spanish regulations on personal data protection (LORTAD) – the following and currently in force is the 1999 LOPD – until the 2010 Mexican Law. This is a jeopardising situation, as the Mexican regulation is in the process of implementation and adaptation, as well as awareness-rising of the population. This vulnerability is also due to the absence of an appropriate law and jurisdictional delimitation of the right, which is not surprising given its recent introduction to the legislation.

The right of personal data protection makes its first appearance in Mexico in 2002, in the Federal Law for Transparency and Access to Government Public Information; and later on, in the 2009 Constitutional Reforms of the articles 16 and 73. The legislative evolution comes to an end with the recent publication of the 2010 Federal Law for the Protection of Personal Data in possession of private individuals, and its Regulations in 2011. This first appearance lacked effectiveness. At that time, indeed, it related to the Law of Transparency for the Protection of Personal Data in possession of the public administration, yet not of private individuals, as it is nowadays.

Incidentally, this brief regulation to the data protection right appeared in Mexico in 2002, in the same year of the Transparency Law. Therefore - given the corruption legacy of this country – it was mainly aimed at the objectives of this Law, namely the transparency and the access to public information. Hence, the right of personal data protection did not evolve appropriately. Now that the right of transparency is in its maturity stage, the current societal needs call for the consolidation of the right of personal data protection in order to endow the individual with the right to dispose of his/her own private information.

As the analysis reveals - as a product of the historic links of cooperation with Spain - the Mexican Law has been clearly affected by the remarkable influence of the Spanish experience, as well as by the main discussion topics among specialists. These points of discussion derive from the latest technology advances, which include new information storing resources such as *cloud computing* (art.52 RLOPD), whose regulation is problematic given the lack of standardized international legislations. Similarly, the same consideration applies to the case of the clarification of the Law regarding the right of objection (articles 8 and 27 LPDP), which is a clear rectification in the Mexican Law; and whose omission in the Spanish Law raised some criticism (articles 34-36 RLOPD).

In spite of its tardiness, nowadays the importance of the fundamental right of personal data protection is recognised in Mexico, which is currently endowed with specific Law and Regulations. As a consequence, the enforcement of the right on behalf of its holders is crucial for its implementation. However, the exercise of this right will shine by its absence as long as individuals are not aware of the rights and the legal actions they are granted.

The principles to be respected by the responsible parties fulfil the current needs and comply with the international requirements. However - since the regulations of personal data protection in possession of the public sector and of the private sector differ – an appropriate unification of the two regulations is necessary in order to clarify the legal principles of this right to the benefit of the users.

As far as the principle of consent is concerned, two types are provided: express consent and implied consent. Unlike in other countries, the latter is a Mexican innovation, consisting in the consent which applies when the holder of the right raises no objection upon being informed of the privacy notice. As a general rule, the implied consent is valid unless the express consent is required by law (articles 13-14 RLPDP). However, given the novelty of this typology, the regulation is not clear as for the mechanism to be followed in the privacy notice itself, for the beholder to state his/her refusal to the data processing.

Likewise - in order to establish international certifications in this area - it is important to create a similar validity mechanism on a national level, regulated by the Institute, whose licence is to be granted to specialised-technical professionals in this sector. This will pave the way to a prompt homogenization of data protection processing. As a consequence, it will enhance the interest of the legal community, fostering the enforcement of the LPDP, as well as boosting the international cooperation and participation in this field.

According to Mexican Law - unlike the Spanish one – the regulatory authority do not provide a register of filing systems, which may turn the person appointed to this task into a risk for the individual. If the person in charge of data collection is not well-aware of the Law and correctly informed of the information that can be processed – which is not unlikely when implementing a new regulation – there may be the risk of creating excessive databases and information processing. In this case, database applications can be a preventive measure in order not to store personal data in sensitive databases, which may turn to be illegal in the future.

The Mexican regulation does not provide the implementation of different security levels depending on the type of personal data to be processed. The measures provided in the Regulations can give rise to doubt. As a consequence, it is advisable to establish a specific tool for the standardization of different security levels to be complied with by the person appointed to this task.

The presence of a person in charge of the enforcement of the data protection regulation, in every company and Institution, is important for the appropriate implementation of the Law. In addition, this practice will enhance job creation and professional specialization in this area.

In the Mexican case (articles 64-66 LPLP), the fine scheme is higher than the Spanish one, despite the Law significantly mentions that the competent authority will have to take “the financial capacity of the liable party” into account. On the other hand, personal data undue processing-related crimes are classified under the data protection Law itself. Both situations intrinsically enhance the Law enforcement. Nevertheless – since it is a recent law – as long as

the fines and the crime classification are not carried out, not only the regulation will not be implemented, but it will also be deliberately vulnerable.

The crime classification (personal data undue processing-related crimes) - in Chapter XI of the Federal Law for personal data protection in possession of private individuals - regulating the special crimes in this area, is interesting and appropriate. This is an innovation of the Mexican law, since it is not classified in the equivalent Laws in countries such as Spain, Argentina, Costa Rica, and Peru.

Habeas data is a constitutional guarantee implemented in Latin American countries, whose main distinctiveness is that it is appealed before a Judicial Body, and it is not an administrative procedure, as it is in European countries. This is a consequence of the historical necessities typical of the dictatorial systems of governance which took place in Latin America.

The necessity of the guarantee granted by an administrative body specialised in this area is deemed appropriate. On the other hand - mainly in order to reinforce the fundamental right - it is equally advisable that the *Habeas Data* is to be appealed to in Mexico only in maximum security situations such as the ones dealing with sensitive data, security and defence of large communities, as well as regarding evident national interests.

Finally, an awareness-raising campaign by the Institute is advocated, in order to educate the population about this right and how to avail of it. Therefore, the IFAI will issue resolutions to be implemented before the Federal Judicial Authority; whose rulings will constantly clarify and classify this new right.

Glosario

AEPD	Agencia Española de Protección de Datos
AN	Audiencia Nacional de España
ARCO	Acceso, Rectificación, Cancelación y Oposición.
Art.	Artículo
Arts.	Artículos
ASN	Autoridad Sanitaria Nacional
CDF	Carta de los Derechos Fundamentales de la Unión Europea
CE	Consejo de Europa
CE	Constitución de España
CECA	Comunidad Europea del Carbón y del Acero
CEDH	Convenio Europeo de Derechos Humanos
CEPC	Centro de Estudios Políticos y Constitucionales
CIDH	Carta Internacional de los Derechos Humanos
CNPD	Comisión Nacional de Protección de Datos
CNPDPI	Comisión Nacional de Protección de Datos Personales Informatizados
CPEUM	Constitución Política de los Estados Unidos Mexicanos
CPM	Constitución Política de México
CURP	Clave Única de Registro de Población en México
DADDH	Declaración Americana de los Derechos y Deberes del Hombre
DF	Distrito Federal
DI	Derecho Internacional
DIC	Derecho Internacional Común
DIDH	Derecho Internacional de los Derechos Humanos
DOF	Diario Oficial de la Federación
DUDH	Declaración Universal de los Derechos Humanos
FESP	Funciones Esenciales de Salud Pública
FFJJ	Fundamentos Jurídicos
FJ	Fundamento Jurídico
IFAI	Instituto Federal de Acceso a la Información y Protección de Datos

IIJ	Instituto de Investigaciones Jurídicas de la Universidad Nacional Autónoma de México
INTECO	Instituto Nacional de Tecnologías de la Comunicación
IP	<i>Internet Protocol</i>
LAI	Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental en México
LO	Ley Orgánica de España
LOPD	Ley Orgánica de Protección de Datos de Carácter Personal en España
LORTAD	Ley Orgánica de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal
LPDP	Ley Federal de Protección de Datos Personales en posesión de los particulares.
Num.	Número
OEA	Organización de Estados Americanos
ONU	Organización de las Naciones Unidas
OPS	Organización Panamericana de la Salud
Párr. /Pár.	Párrafo
PDP	Protección de Datos Personales
RA	Recurso de Amparo
RAE	Real Academia Española
RD	Real Decreto de España
RFC	Registro Federal de Contribuyentes
RLPDP	Ley Federal de Protección de Datos Personales en posesión de los particulares.
SA	Sociedad Anónima
SAN	Sentencia de la Audiencia Nacional
SCJN	Suprema Corte de Justicia de la Nación en México
SSTC	Sentencias del Tribunal Constitucional de España
STC	Sentencia del Tribunal Constitucional de España
STEDH	Sentencia del Tribunal Europeo de Derechos Humanos
STS	Sentencia del Tribunal Supremo de España
TC	Tribunal Constitucional de España

TEDH	Tribunal Europeo de Derechos Humanos
TJCE	Tribunal de Justicia de la Comunidad Europea
TS	Tribunal Supremo de España
UE	Unión Europea
UNAM	Universidad Nacional Autónoma de México
Vol.	Volumen

0. INTRODUCCIÓN

Hoy en día no es tarea fácil mantenerse en un moderado anonimato, sin que por él nos encontremos en el riesgo de ignorar lo que de nuestra persona es público para otros y cuya publicidad no hemos autorizado. Sin embargo, lo que sí es posible, es gestionar nuestros datos personales responsablemente para contribuir a la protección de nuestros derechos. Esta reflexión, tiene que ver con nuestra vida virtual, que cada vez más es casi imposible resistirse a tenerla, debido al sistema actual de interacción social. Ahora mismo, es extraño que una persona con una serie de actividades normales no aparezca en la red. Esta situación hace que el reciente derecho a la protección de datos personales, presente infinidad de dudas, así como nuevos problemas y escenarios para ejercerlo y garantizarlo.

En la actualidad es cada vez más común enterarse a través de distintos medios de comunicación, de la existencia de graves violaciones a la privacidad de las personas, y que se han incrementado a partir de los avances tecnológicos, así como del uso creciente de las redes sociales mediante internet. Esto se debe a que las actividades que se desarrollan a cada instante dejan un rastro -invisible a simple vista- de quiénes somos, qué hacemos, dónde estamos, cuáles son nuestros hábitos y preferencias, así como muchos otros datos más, que al ser asociados por sistemas informáticos proporcionan un retrato fiel de cada individuo.

Así, la vida de las personas gira en torno a proporcionar (consciente o inconscientemente, obligatoria o voluntariamente) datos personales como el nombre, edad, estado civil, historial crediticio, cuentas bancarias, trayectoria educativa, estado de salud, color de piel, etc. Lo anterior, es producto de realizar: pagos, compras, aperturas y cancelación de cuentas, depósitos bancarios, consultas médicas, solicitudes de información, movimientos a través de internet, entre muchas otras operaciones. En este sentido, es cierto que Internet ha logrado facilitar inmensurablemente las actividades diarias en el trabajo, estudios, comercio, etc. Sin embargo, también ha traído consigo graves problemas de invasión a la privacidad, asociados principalmente al uso indebido de los datos personales y del incorrecto tratamiento por parte de quiénes los poseen.

La protección de datos personales es un derecho de los llamados de tercera generación, con orígenes marcadamente europeos, y que ha tenido en las últimas tres décadas una rápida evolución, principalmente por el uso de Internet. Este derecho garantiza a la persona un poder de control y disposición sobre sus datos personales, permitiéndoles consentir su recogida y uso, así como a saber quién los posee y con qué finalidad.

En estos primeros párrafos pareciera que el derecho a la protección de datos personales únicamente tiene que ver con datos automatizados, pero no es así, también comprende los ficheros manuales en cuyo proceso de recopilación o tratamiento no existe fase automatizada alguna. Sin embargo, y dada la era de globalización y tecnología en la que actualmente se encuentra inmersa la sociedad estas situaciones son cada vez más escasas, y aparentemente más inofensivas. La realidad es que tanto los ficheros automatizados como manuales representan el mismo riesgo para el individuo, la única diferencia radica en que los manuales están desapareciendo por el esfuerzo y el tiempo que significan para el encargado del tratamiento, mientras que los automatizados han aumentado. Estos últimos ficheros, son más fáciles de manipular a la hora de trabajar con ellos o de efectuar el tratamiento de diversa información, asimismo, es más sencillo realizar una transferencia de datos personales. Por ello, las bases de datos automatizadas son altamente susceptibles de errores humanos y/o de programación que ponen en riesgo al individuo, mediante la intrusión de amenazas de muy diversa índole (hackers, problemas de seguridad en el acceso, tratamiento inadecuado, destrucción inadecuada, revelación de información, etc.).

Tanto en México como en América Latina, España ha sido un país de gran influencia debido a los fuertes lazos de cooperación forjados a lo largo de la historia. En consecuencia, el ámbito jurídico no ha sido la excepción. Por tanto, no es de extrañar, que a partir de la LORTAD y de la actual LOPD, el desarrollo de la normatividad referente al derecho de protección de datos personales haya evolucionado, repercutiendo en el surgimiento de legislaciones similares en países como Argentina, Colombia, Costa Rica, Perú y México.

El derecho a la protección de datos personales es un derecho de origen europeo y España es uno de los países más evolucionados gracias al trabajo de la Agencia Española de Protección de Datos (órgano garante y especializado en la materia), así como, por el trabajo efectuado por las Agencias de las distintas Comunidades Autónomas. Instituciones, las anteriores, a las cuales se les tiene encomendada la garantía de este derecho, además de una labor extremadamente importante que es su difusión como derecho de reciente configuración.

En este sentido, el propósito de esta investigación es el estudio del derecho fundamental a la protección de datos personales en México, desde el análisis de la legislación española. Así, intentaré presentar una perspectiva global de este nuevo derecho fundamental en México, analizando su origen europeo y la necesidad de la realidad actual que ha llevado al país a la importación de este nuevo derecho fundamental, así como los mecanismos de garantía instituidos por la Ley de la materia. De igual manera, se analizarán algunos de los retos que la regulación normativa presenta, y no solo por su reciente configuración, sino porque la misma no resuelve los problemas propios que emergen de la realidad actual en la que la sociedad se desarrolla.

Para la elaboración de la presente investigación se ha utilizado el método analítico-comparativo del derecho a la protección de datos personales, para proporcionar una perspectiva del estado actual de este derecho fundamental en México. Así, Este trabajo se ha elaborado a partir del estudio del derecho español, observando los avances legislativos que México ha tenido durante los últimos años, que a partir de 2009, han sido bastantes significativos dadas las reformas constitucionales acaecidas. Afortunadamente y desde 2010, México cuenta con una Ley Federal de Protección de Datos Personales en posesión de particulares.

Sin embargo, este notable retraso en la emisión de la Ley vuelve al país vulnerable ante la protección y garantía de este derecho. Esto, no solo es así por lo que implica el arduo proceso de implementación de una ley, sino porque además ha de lidiar con los avatares propios que de los vertiginosos avances de la tecnología y la transmisión de la información, a la que se enfrentan países maduros en este tema como es el caso de España. De manera que hacer una tesis

sobre estos temas, conlleva la inherente realidad de no agotar el tema debido a la nueva normativa, parámetros, recomendaciones, etc. que surgen en torno a esta disciplina, pero que es increíblemente útil para la construcción del conocimiento a la hora de proponer nuevas soluciones. Ahora bien, y para este trabajo en lo que concierne al caso mexicano se han tomado en consideración los principales documentos legislativos surgidos hasta Octubre de 2012.

Así entonces, el presente estudio se compone de cuatro capítulos. El primero lo hemos titulado: origen y evolución del derecho a la protección de datos personales. En el se abordan elementos importantes para la comprensión del tema, como aquellos relacionados con el origen del derecho a la protección de datos, que tiene su génesis en el estudio del derecho a la privacidad, mismo que halla su fuente en diversos instrumentos internacionales de protección de los derechos humanos. Así, observaremos cómo desde la Declaración Universal de Derechos Humanos queda instituido el derecho a no ser objeto de injerencia en nuestra vida privada, familia, domicilio o correspondencia, y culminaremos con el estudio del primer instrumento que reconoce distintos derechos innovadores de última generación, como es el caso del tema que hoy nos ocupa.

El segundo capítulo se titula: el derecho a la protección de datos personales y sus primeras inserciones constitucionales. En este apartado discutimos algunas definiciones provenientes de los ámbitos doctrinario y constitucional, prestando particular atención en aquellas derivadas de la doctrina generada por el Tribunal Constitucional español. La naturaleza de este derecho es otro de los temas abordados, en particular nuestro capítulo se ocupa de analizar los principales argumentos en torno a la autonomía del derecho a la protección de datos personales. Asimismo, se estudian conceptos básicos para el análisis de nuestro tema, tales como: privacidad, intimidad, el bien jurídico protegido, derecho a la información y hábeas data. El apartado concluye haciendo referencia a la inserción constitucional realizada por los países pioneros en la materia como son Portugal, Alemania y Francia, además incluimos el caso español por ser referente permanente para nuestro objeto de estudio.

En el tercer capítulo, denominado la protección de datos personales en España, además de hacer una descripción del trabajo elaborado por las autoridades en la materia, realizamos una útil recopilación de la evolución jurisprudencial de este derecho en la doctrina del Tribunal Constitucional español. El apartado culmina con un estudio hecho a partir de la doctrina académica y jurisdiccional española, en lo que hace al objeto, función, titulares, contenido, tipo de datos, derechos de las personas, límites, tratamiento, principios y normas legales reguladoras.

Finalmente, el cuarto capítulo corresponde al derecho a la protección de datos personales en México. Es importante mencionar que en la actualidad y por motivos de nueva incorporación, el país no se cuenta con un gran acervo doctrinario, como si ocurre en España. Por ello, el presente estudio tiene como finalidad proporcionar las bases teóricas y prácticas vistas desde la experiencia española. De esta manera y siguiendo la estructura del capítulo correspondiente a España, desarrollamos el análisis de la nueva legislación mexicana en lo que hace a la definición, sujetos, objeto, límites del derecho, atribuciones de la Autoridad garante, principios del derecho en lo que hace al sector público, así como aquellos correspondientes al sector privado, terminando con los derecho y la normatividad aplicable en materia de protección de datos personales.

El siguiente epígrafe de nuestro trabajo recoge algunas conclusiones que hacen énfasis a los retos que habrá de enfrentar la Ley Federal de Protección de Datos Personales, para lograr una rápida y adecuada evolución, que sitúe a México en un nivel de garantía similar al de las naciones más avanzadas en la materia. Asimismo, se hace un análisis comparativo de las normas en lo que hace a figuras nuevas en la legislación mexicana, y se señalan ciertas características de la misma que crean cierta confusión.

Después de la sistematización bibliográfica utilizada para la presente tesis, hemos agregado un último apartado denominado “Anexos” que corresponde a la experiencia práctica llevada a cabo desde el Instituto antes de que se dictara la Ley Federal de Protección de Datos Personales en posesión de particulares, que

tiene que ver con los datos en posesión de los sujetos obligados, es decir de la Administración Pública Federal.

Finalmente, concluyo esta introducción esperando que después de la lectura de este trabajo de investigación, el lector tenga un panorama suficientemente amplio de la situación actual del derecho a la protección de datos personales en México a partir de su aparición en Europa y su posterior evolución en España, hasta su actual reflejo en el ámbito jurídico mexicano.

0. INTRODUZIONE

Oggigiorno non è facile mantenere un moderato anonimato, senza dover correre il rischio di non venire a conoscenza di ciò che della nostra persona diventa pubblico e di quale pubblicità non abbiamo dato l'autorizzazione. Ciò nonostante è possibile gestire i nostri dati personali con responsabilità per contribuire alla tutela dei nostri diritti. Questa riflessione coinvolge la nostra vita virtuale, a cui è sempre più difficile sottrarsi per via dell'attuale sistema di interazione sociale. Al giorno d'oggi, risulterebbe strano che una persona con una serie di attività normali non appaia nella rete. Tale situazione fa sì che il recente diritto alla protezione dei dati personali presenti un'infinità di dubbi, nuovi problemi e scenari con cui esercitarlo e gestirlo.

Attualmente, è sempre più comune venire a conoscenza, attraverso diversi mezzi di comunicazione, dell'esistenza di gravi violazioni alla privacy personale, le quali sono aumentate di pari passo con i progressi tecnologici e il crescente uso dei social network di internet. Ciò è dovuto al fatto che ogni attività nella rete lascia una traccia – invisibile alla vista – di chi siamo, cosa facciamo, dove siamo, quali sono le nostre abitudini e preferenze, così come molti altri dati, i quali essendo associati a sistemi informatici, forniscono un ritratto fedele di ogni individuo.

In questo modo, la vita delle persone ruota attorno alla diffusione (cosciente o inconsciente, obbligatoria o volontaria) di dati personali come il nome, l'età, lo stato civile, registri creditizi, conti bancari, carriera accademica, stato di salute, colore della pelle, ecc. Tutto ciò è dovuto a: pagamenti, spese, apertura e cancellazione di conti, depositi bancari, consulenze mediche, richieste di informazione, movimenti su internet, e molte altre operazioni. In questo senso, è innegabile che internet sia riuscito a facilitare enormemente le attività giornaliere nel lavoro, nello studio, nel commercio, ecc. Cionondimeno, ha comportato anche gravi problemi d'invasione della privacy, legati principalmente all'uso indebito dei dati personali e alla gestione scorretta da parte di chi li possiede.

La tutela dei dati personali è uno dei cosiddetti diritti di terza generazione, dalle origini tipicamente europee, che ha avuto una rapida evoluzione nelle ultime tre decadi, dovuta principalmente all'uso di internet. Tale diritto garantisce alla persona un potere di controllo e disposizione in merito ai propri dati personali, permettendo il consenso alla loro raccolta e uso, così come la conoscenza di chi li possiede e con quali finalità.

Questi paragrafi potrebbero dare l'erronea impressione che il diritto alla tutela dei dati personali ha unicamente a che fare con i dati automatizzati. Questi ultimi, al contrario, comprendono anche i formulari manuali nel cui processo di compilazione o trattamento non esiste alcuna fase automatizzata. Ciò nonostante, data l'era della globalizzazione e della tecnologia in cui è attualmente immersa la società, queste situazioni sono sempre più scarse e inoffensive. In realtà, sia i formulari manuali che quelli automatizzati rappresentano lo stesso rischio per l'individuo. L'unica differenza risiede nel fatto che quelli manuali stanno scomparendo per via dello sforzo e del tempo che comportano all'incaricato del loro trattamento, mentre quelli automatizzati sono aumentati. Questi ultimi sono di più facile manipolazione qualsiasi sia il tipo di trattamento nei loro confronti, sebbene risulti più facile realizzare un trasferimento di dati personali. Per questo motivo, i database automatizzati sono altamente suscettibili a errori umani e/o di programmazione, che mettono a repentaglio l'individuo attraverso l'intrusione di minacce di diverso tipo (hackers, problemi di sicurezza durante l'accesso, trattamento inadeguato, distruzione inadeguata, rivelazione di informazioni, ecc.).

Per il Messico come per l'America Latina, la Spagna è stato un paese di grande influenza per via dei forti legami di cooperazione storici, e l'ambito giuridico, di conseguenza, non ha fatto eccezione. Non c'è da stupirsi, pertanto, che dalla LORTAD all'attuale LOPD, l'evoluzione delle normative relative al diritto di protezione dei dati personali si sia sviluppata ripercuotendosi nella creazione di legislazioni simili in paesi come Argentina, Colombia, Costa Rica, Perù e Messico.

Quello della protezione dei dati personali è un diritto di origine europea, e la Spagna è uno dei paesi più evoluti in questo settore grazie all'attività della

Agencia Española de Protección de Datos (Organo garante e specializzato in materia), insieme al lavoro svolto dalle *Agencias* delle diverse Comunità Autonome, e Istituzioni cui si affida la garanzia di tale diritto, oltre all'onere della sua diffusione in quanto diritto di recente introduzione.

In tal senso, l'obiettivo di questa ricerca è lo studio del diritto fondamentale alla protezione dei dati personali in Messico, in base all'analisi della legislazione spagnola. Mi propongo dunque di presentare una prospettiva globale di questo nuovo diritto fondamentale in Messico, analizzando la sua origine europea e la necessità della realtà attuale che ha portato tale diritto fondamentale all'attenzione di questo paese, così come i meccanismi di garanzia istituiti dalla Legislazione in materia. Allo stesso modo, saranno analizzati alcuni degli obiettivi che la regolazione normativa presenta, non solo per la sua recente configurazione, ma anche perché questa non risolve i problemi presenti nell'attualità del mondo in cui la società si evolve.

Per l'elaborazione della presente ricerca è stato usato il metodo analitico-comparativo del diritto alla protezione dei dati personali, al fine di fornire una visione complessiva dello stato attuale di questo diritto fondamentale in Messico. Tale ricerca è stata dunque elaborata in base allo studio della giurisdizione spagnola, osservando i progressi legislativi che hanno interessato il Messico negli ultimi anni, i quali sono stati molto significativi dal 2009, per via delle riforme costituzionali in materia. Dal 2010 fortunatamente, il Messico conta di una Legge Federale per la Protezione dei Dati Personali in possesso dei soggetti privati.

Ciò nonostante, questo considerabile ritardo nell'emissione della Legge rende il paese vulnerabile in merito alla protezione e alla garanzia di questo diritto. Ciò non è solamente dovuto al difficile processo d'implementazione della legge, ma perché ha a che fare con i cambi propri dei vertiginosi progressi della tecnologia e della trasmissione d'informazione, che coinvolgono i paesi maturi in questo settore, come la Spagna. Di conseguenza, una tesi in questo ambito comporta l'inerte eventualità di non riuscire a soddisfare pienamente l'oggetto della ricerca per via delle nuove normative, parametri, raccomandazioni, ecc. che

influenzano una disciplina del genere. Ciò risulta tuttavia un mezzo immensamente valido per la conoscenza della materia in vista di proposizioni di nuove soluzioni. Per quanto riguarda il caso messicano, ai fini della presente ricerca sono stati presi in considerazione i principali documenti legislativi redatti fino all'Ottobre del 2012.

La presente ricerca è dunque composta di quattro capitoli. Il primo s'intitola: "Origine ed evoluzione del diritto alla protezione dei dati personali" in cui vengono trattati elementi importanti per la comprensione dell'oggetto della tesi, come quelli relativi all'origine del diritto alla protezione dei dati, che derivano dallo studio del diritto della privacy, sebbene siano fondati in diversi strumenti internazionali per la protezione dei diritti umani. Osserveremo quindi come dalla Dichiarazione Universale dei Diritti Umani viene istituito il diritto a non essere oggetto di ingerenze nella nostra vita privata, famiglia, domicilio o corrispondenza. Termineremo infine con lo studio del primo strumento che riconosce diversi diritti innovativi di ultima generazione, come l'oggetto della presente ricerca.

Il secondo capitolo s'intitola: il diritto alla protezione dei dati personali e le sue prime apparizioni costituzionali. Saranno qui discusse alcune delle definizioni provenienti da ambiti dottrinali e costituzionali, con particolare attenzione a quelle derivanti dalla dottrina generata dal Tribunale Costituzionale spagnolo. La fenomenologia di questo diritto è un altro tema oggetto della presente ricerca. Questo capitolo in particolare analizza i principali argomenti relativi all'autonomia del diritto alla protezione dei dati personali. Saranno inoltre studiati i concetti basilari per l'analisi di questo tema, come: privacy, riservatezza, il bene giuridico protetto, il diritto all'informazione e l'*habeas data*. In conclusione, si farà riferimento all'introduzione costituzionale realizzata da paesi pionieri in materia, come Portogallo, Germania e Francia. Sarà inoltre incluso il caso spagnolo poiché referenza permanente per il nostro oggetto di studio.

Nel terzo capitolo, con il nome "protezione dei dati personali in Spagna", oltre alla descrizione del lavoro elaborato dalle autorità in materia, sarà realizzata un'utile ricompilazione dell'evoluzione giurisdizionale di tale diritto nella

dottrina del Tribunale Costituzionale spagnolo. Il capitolo termina con lo studio della dottrina accademica e giurisdizionale spagnola, in merito a oggetto, funzione, titolari, contenuto, tipo di dati, diritti della persona, limiti, trattamenti, principi e norme legali regolatrici.

Infine, il quarto capitolo ha come oggetto il diritto alla protezione dei dati personali in Messico. È importante notare come oggigiorno per via della sua nuova introduzione, questo paese non conta su di un'importante eredità dottrina, come è il caso della Spagna. Di conseguenza, la presente ricerca mira a fornire le basi teoriche e pratiche viste dal punto di vista dell'esperienza spagnola. In questo modo, e seguendo la stessa struttura del capitolo relativo alla Spagna, sarà analizzata la nuova legislazione messicana in quanto a definizione, soggetti, oggetto, limiti del diritto, attribuzioni dell'Autorità garante, principi del diritto riguardanti il settore pubblico, e le relative corrispondenze nel settore privato. Si concluderà con il diritto e le normative applicabili in materia di protezione dei dati personali.

La successiva epigrafe di questo studio raccoglie alcune conclusioni che sottolineano gli obiettivi che la Legge Federale per la Protezione dei Dati Personali si dovrà prefiggere per un'evoluzione rapida e adeguata, che posizioni il Messico a un livello di garanzia simile a quello delle nazioni avanzate in materia. Sarà inoltre compiuta un'analisi comparativa delle norme relative a nuove figure nella legislazione messicana, e saranno segnalate alcune caratteristiche delle stesse che possono risultare motivo di confusione.

Dopo l'esposizione bibliografica utilizzata per questo studio, è stato inserito un ultimo paragrafo denominato "Annessi" corrispondente all'esperienza pratica realizzata nell'Istituto prima che fosse redatta la Legge Federale per la Protezione dei Dati Personali posseduti da soggetti privati, che riguardano i dati in possesso dei soggetti obbligati, ovvero l'Amministrazione Pubblica Federale.

Concludo infine questa introduzione nella speranza che, dopo la lettura della presente ricerca, il lettore acquisisca una visione d'insieme sufficientemente ampia della situazione attuale del diritto alla protezione dei dati personali in

Messico a partire dalla sua apparizione in Europa e la sua successiva evoluzione in Spagna, fino al suo attuale riflesso nell'ambito giuridico messicano.

I. ORIGEN Y EVOLUCIÓN DEL DERECHO A LA PROTECCION DE DATOS PERSONALES

En el presente capítulo se abordarán las nociones de derechos fundamentales y derechos humanos, así como la descripción de los instrumentos internacionales que a lo largo de los años han ido perfilando el derecho a la protección de datos personales, primero mediante el derecho a la privacidad, para luego configurar un derecho a parte que es la protección de datos personales.

En primer lugar, es importante referir las definiciones de los conceptos a los que se hará referencia constantemente y antes de entrar con el tema del derecho fundamental a la protección de datos personales, es esencial revisar las nociones de derecho humano y derecho fundamental, ya que es básico diferenciar uno de otro para posicionar nuestro tema de estudio.

El primer antecedente del derecho a la protección de datos, se encuentra en el derecho a la privacidad, que protege la vida privada y familiar. Este último, es reconocido internacionalmente desde 1948. Por ende, posee un bagaje histórico más amplio en lo que respecta a los ordenamientos internacionales y regionales que lo garantizan. Por lo anterior, se ha considerado importante citar los artículos correspondientes en cada uno de los instrumentos internacionales, y para una mayor comprensión, se hace una breve anotación descriptiva de los mismos¹.

El derecho a la protección de datos personales tiene como finalidad la autodeterminación informativa, es decir que la persona disponga libremente de la utilización de sus datos y de esta manera pueda proteger su vida privada. Esto último, podría dar indicios para pensar que no es un derecho autónomo, sino que forma parte del derecho a la privacidad; sin embargo, esta idea no tiene ahora mismo sustento, es una idea superada por la doctrina actual que define a la protección de datos como un derecho autónomo.

¹ Sección descriptiva –de instrumentos internacionales– que resulta de interés, porque con ésta se logran apreciar las principales características y diferencias entre los ordenamientos, así como el contenido que se reitera y los objetivos para los cuales fueron creados. Estos son datos que en cualquier estudio, son siempre interesantes y facilitan la comprensión.

1. Derechos humanos y derechos fundamentales

La denominación de *derechos humanos* presenta diferentes variantes léxicas, dependiendo de las tendencias doctrinales del momento. Se pueden encontrar como derechos fundamentales, derechos naturales, derechos subjetivos, derechos públicos subjetivos o libertades públicas². Actualmente, los términos más utilizados son “derechos humanos” o “derechos fundamentales”, que si bien comparten contenido en tanto que se ocupan de reconocer los derechos inherentes a la persona, hacen referencia a los diferentes ámbitos de aplicación, ya que por el primero se entiende el espacio internacional, mientras que el segundo apunta a la esfera nacional.

El término *derechos fundamentales* «*droits fondamentaux*», aparece en Francia hacia 1770 con el movimiento político y cultural que condujo a la Declaración de los Derechos del Hombre y del Ciudadano de 1789. Sin embargo, en ésta son referidos como *derechos naturales*³, inalienables, sagrados y de observancia para los poderes públicos. La expresión de *derechos fundamentales*, ha alcanzado especial relieve en Alemania, donde bajo el título de “derechos fundamentales” «*Grundrechte*» se ha articulado el sistema de relaciones entre el individuo y el Estado, en cuanto fundamento de todo el orden jurídico-político, este es su sentido en la “Ley Fundamental” «*Grundgesetz*» de Bonn de 1949. De ahí, que gran parte de la doctrina entienda que los *derechos fundamentales* son

² Por no ser materia principal de este estudio, no se entrará al análisis de cada uno de los términos. Sin embargo, se considera importante aclarar que todas estas variantes léxicas, al final solo se refieren a cuestiones filosóficas y/o de formalidad, y en general coinciden en la esencia de lo que significan los derechos esenciales para la persona.

³ Decimos que los derechos fundamentales aparecen en este instrumento con el nombre de “derechos naturales”, por ser plasmados formalmente y por primera vez en un documento, para convertirse en derecho positivo de la época. Esta Declaración es anterior al constitucionalismo moderno y las primeras Constituciones garantistas de derechos fundamentales. La Constitución mexicana de 1917 es la primera que introduce los derechos sociales en esta nueva etapa de constitucionalismo moderno, seguida por Weimar en 1919. Para referir un antecedente más lejano, solo por abundamiento, la Carta Magna de 1215 y otorgada por el Rey Juan I de Inglaterra (Juan sin Tierra), contemplaba cierta seguridad jurídica para las personas y comerciantes, y proclamaba el respeto de algunos derechos como la libertad religiosa y política. Sobre la Carta Magna puede consultarse a Pegoraro et al. (2000: 441-443). Con relación a los derechos reconocidos constitucionalmente, Pachot (2010: 38) considera que en un principio, deben considerarse con el mismo valor jurídico de fundamentales, pudiendo diferenciarse por el grado de protección jurídica destinado a los mismos en el ordenamiento jurídico respectivo. Y que de tal modo, deben delimitarse dos cuestiones diferentes: el reconocimiento (existencia) de un derecho y, por otra parte, el grado de protección que recibe el mismo.

aquellos *derechos humanos positivizados* en las constituciones de cada país (Pérez Luño, 1999: 30-31). Los derechos fundamentales, suponen uno de los aspectos del desarrollo del individualismo y del protagonismo que adquiere el hombre individual, en el nuevo orden económico y social que surge en el tránsito a la modernidad (Peces-Barba Martínez, 1982: 6).

Los *derechos humanos*, surgen en su máximo esplendor el 10 de Diciembre de 1948, con la Declaración Universal de Derechos Humanos, producto de la segunda guerra mundial. La Declaración recoge algunos derechos fundamentales que estaban establecidos en distintas Constituciones, que eran ejercidos frente al Estado y protegidos por éste. Es en este momento, que los derechos humanos surgen como tales, entendidos antes como “derechos naturales” (ideal filosófico, por ser propios de la naturaleza humana), que al ser positivizados se convierten en lo que se denomina hoy como “derechos fundamentales”. Es decir, los derechos humanos, surgen después de que la Asamblea de Naciones Unidas, máximo representante de la comunidad internacional, aprueba la Declaración; para que no solamente fuesen reconocidos por el Estado, sino también, ejercidos contra éste, en el caso de que dejase de cumplir con su obligación de protección (Bobbio, 1991:39)⁴.

Hoy en día, las declaraciones de derechos humanos, ya sean universales, regionales o internas en un país determinado, tienen el carácter de postulados básicos de convivencia social que se proponen como premisa “política” de una vida en sociedad. Cuando cuentan con un consenso universal, tienen dentro del

⁴ Bobbio (1991: 39), recuerda lo dicho por Locke y los iusnaturalistas cuando afirmaban que: “los derechos naturales eran pura y simplemente teoría filosófica, que no tenía otro valor que el de una exigencia ideal, el de una aspiración que había podido ser realizada sólo cuando alguna constitución la hubiese acogido y transformado en una serie de prescripciones jurídicas. En un segundo momento, la afirmación de la existencia de los derechos naturales originarios limitadores del poder soberano viene acogida en las declaraciones de derechos que preceden a las Constituciones de los Estados liberales modernos: desde este momento los derechos naturales no son ya solamente una aspiración ideal, sino que se convierten en verdaderas y propias pretensiones jurídicamente reconocidas y protegidas contra eventuales violaciones por parte de los particulares y de los poderes públicos. Con la acogida de algunos derechos fundamentales en la Declaración Universal se cumple el tercer momento de esta evolución: los derechos naturales, reconocidos ya por la Asamblea General de las Naciones Unidas, esto es, por el más alto órgano representativo de la comunidad internacional, tienden a ser protegidos no ya solamente en el ámbito del Estado, sino también *contra el Estado mismo*, es decir, tienden a una protección que se podría llamar de segundo grado, la cual debería entrar en funcionamiento cuando el Estado dejase de cumplir sus obligaciones constitucionales en las relaciones con sus sujetos”.

Derecho Internacional el valor de elementos indicativos y determinados que se llaman “principios generales de derecho reconocidos por las naciones civilizadas”; y por lo tanto, trascienden manifiestamente hacia el campo jurídico, al menos para los fines de ese Derecho Internacional. Sin embargo, por sí mismas no tienen efecto normativo, ni valen para imponer a un Estado el reconocimiento o el respeto de los derechos de quienes viven en su territorio. En cambio, desde el momento en que su contenido se vacía dentro de la legislación positiva de un Estado, adquieren un carácter jurídico y pasan a integrar la legislación positiva de ese país. Con ello, los derechos humanos se convierten en instituciones jurídicas, conforme al alcance que el texto legal concreto les asigne (Novoa Monreal, 2001: 16-17).

Actualmente, se sigue la misma línea establecida para el uso de la terminología de los derechos fundamentales y los derechos humanos. Aunque no existe una regla taxativa para ello, podríamos decir que este último término, es utilizado en el ámbito internacional, como en la Declaración Universal de Derechos Humanos; mientras que la denominación derechos fundamentales, es utilizada internamente en los Estados, tal y como se encuentra establecido en los capítulos correspondientes a los Derechos Fundamentales, de constituciones como la de España, Portugal o Alemania. Cabe destacar la existencia de la Carta de los Derechos Fundamentales de la Unión Europea, instrumento más bien regional, por ser materia vigente solo para los 27 países de la Unión Europea.

2. Generaciones históricas de derechos humanos

La historia de los derechos humanos y sus cambios han determinado la aparición de las diferentes generaciones de derechos que se conocen hoy en día, que nacen con la modernidad y a partir de las revoluciones burguesas del siglo XIII (Pérez Luño, 2006: 27)⁵. El grueso de los estudios en la materia, se decanta

⁵ Al respecto Peces-Barba Martínez (1982: 7) dice que: “las estructuras del poder político medieval son sustituidas por el Estado como forma del poder racional centralizado y burocrático. La aparición del Derecho, como *iustrumentum regni* para acabar con los poderes locales plurales contribuirá también grandemente a la consolidación del Estado. Este Estado que aparece primero como Estado estamental, y por consiguiente, con factores y elementos propios del mundo medieval, se hará después Estado absoluto. La burguesía naciente y el sistema capitalista se ampararán, para fortalecerse, en esa nueva forma política, que favorecerá el desarrollo de esta clase y del sistema económico a ella vinculado, hasta que ya en el siglo XVIII, la fuerza de la

por la existencia de tres generaciones, posición que al momento es la más utilizada y aceptada. Sin embargo, en los últimos años hay diversos autores que se inclinan por la existencia de cuatro generaciones, y esta división es producto de fragmentar la primera en dos generaciones diferentes entre sí.

El criterio histórico o cronológico, es el que ha definido la forma más común de clasificar a los derechos humanos en las diferentes generaciones, y lo hace atendiendo a ciertas circunstancias políticas en un determinado momento de la historia. La teoría más habitual hasta el momento, es la clasificación de los derechos en tres generaciones: 1) La *primera generación* o derechos civiles y políticos; 2) Los derechos de *segunda generación* o derechos económicos, sociales y culturales; y 3) Los derechos de *tercera generación*. Para varios autores, los derechos de *primera generación* no sólo son los primeros derechos que emergen en el panorama, sino además, son los derechos de *libertad* por excelencia, mientras que los derechos de la *segunda generación* responden al valor de la *igualdad*, y aquellos de *tercera generación* tienen como principal valor de referencia a la *solidaridad* (Martínez de Pisón, 1997: 175; Rodríguez Palop, 2002: 79 y Pérez Luño, 2006: 34-35).

2.1 Generalidades de la primera y segunda generación: especial referencia a la privacidad como derecho de primera generación.

La *primera generación* de derechos (libertades negativas) fue fruto de la lucha de la clase capitalista ascendente contra los privilegios feudales y las restricciones comerciales y se trata, por tanto, de libertades “burguesas”. En cambio, los derechos sociales o de *segunda generación*, no surgen de una simple extensión de estas libertades; estos son el resultado de la lucha de los trabajadores organizados contra el Estado y los empresarios, siendo por consiguiente, libertades “obreras” (Contreras Peláez, 1994: 23).

Para Pérez Luño (2006: 28), la distinción entre ambas generaciones es que en la *primera*, los derechos humanos se consideran derechos de defensa de las

burguesía la llevará a reclamar también para sí el poder político. Entonces el individualismo y la filosofía de los derechos fundamentales, junto con los demás elementos de la filosofía liberal, usando como legitimación el iusnaturalismo racionalista, se separarán, combatirán y destruirán a ese Estado absoluto, que primero sirvió a sus intereses”.

libertades del individuo, que exigen la autolimitación y la no injerencia de los poderes públicos en la esfera privada, los cuales se tutelan por su mera actitud pasiva y de vigilancia en términos de policía administrativa. La *segunda generación* por su parte, es la relativa a los derechos económicos, sociales y culturales, mismos que se traducen en derechos de participación y necesitan de la actividad directa del Estado para garantizarlos⁶.

Los autores que sostienen la existencia de cuatro generaciones de derechos humanos, lo hacen bajo el fundamento de dividir la primera generación en dos, es decir, la *primera generación* corresponde a los derechos civiles, mientras que la *segunda* se ocupa de los derechos políticos. Esta idea surge de considerar injustificado el agrupamiento de ambas clases de derechos en una única generación; pues estos dos grupos, no pudieron haber surgido simultáneamente, pues para que nacieran los derechos políticos, hubieron de aparecer primero los derechos civiles⁷.

La primera etapa, se inicia con la era moderna, abriendo paso a un concepto global de los derechos humanos y a la reivindicación, por parte del grupo burgués emergente, de los derechos fundamentales del hombre y del ciudadano de corte liberal individualista, los cuales conformaban la categoría de los derechos *civiles y políticos*, pertenecientes a la primera generación de derechos humanos, que se plasmaron en los principios y normas contenidos en las declaraciones norteamericanas y francesas del último cuarto del siglo XVIII, así como en las constituciones de los Estados que accedieron a la independencia durante el siglo XIX (Carpizo Mc-Gregor, 1993: 271).

Dentro del Sistema Interamericano de protección a los derechos humanos, los derechos civiles y políticos se encuentran consagrados en la Declaración Americana de Derechos y Deberes del Hombre, y en la Convención Americana

⁶ Los derechos de segunda generación, para Pérez Luño (2006: 28) “requieren una política activa de los poderes públicos encaminada a garantizar su ejercicio, y se realizan a través de las técnicas jurídicas de las prestaciones y los servicios públicos”.

⁷ Es decir, para que existiera el derecho de asociación, hubo de existir primero el derecho de reunión.

sobre Derechos Humanos⁸. En estos instrumentos se encuentran derechos que protegen: la personalidad jurídica, la vida, la integridad personal, la libertad personal, el debido proceso legal o garantías judiciales, la honra (también conocido como derecho al honor⁹), la *privacidad*, la libertad de conciencia y religión, la libertad de expresión, la rectificación o respuesta, de reunión, la libertad de asociación, la nacionalidad, la circulación y residencia, los derechos políticos, el derecho a un recurso sencillo y rápido, etc.

El estudio de la privacidad, parte de un derecho pasivo proclamando la “no injerencia en la vida privada” del individuo y se sitúa en el catálogo de los derechos de primera generación. Este derecho llega a reivindicar un derecho de libertad informática o control de los datos personales incluidos en un fichero informático. Para Conde Ortiz (2006: 27-28) la doctrina distingue tres generaciones de derechos humanos: a) En la primera se configuran las libertades individuales frente a la injerencia de los poderes públicos, exigiendo sus límites y se tutelan por la observancia de derechos individuales; b) En la segunda, desde el Estado Social de Derecho frente al Estado Liberal de Derecho, los derechos económicos, sociales y culturales exigen una política activa que garanticen su ejercicio; y c) En una tercera generación, se incluye la libertad informática como un nuevo derecho del individuo a tutelar su propia identidad informática, concretándose en las garantías de acceso y control de las informaciones procesadas en bancos de datos por parte de las personas a las que conciernen, es decir, aquella que es titular de dicha información.

Para Davara Fernández de Marcos (2011: 44), la privacidad es un término que se utiliza para referirse al perfil que se puede obtener de una persona con el tratamiento de sus datos de carácter personal y que el individuo tiene derecho a exigir que permanezca en su esfera interna, en su ámbito de privacidad.

⁸ Arts. 3 a 25 de la Convención Americana sobre Derechos Humanos o Pacto de San José, suscrita el 22 de noviembre de 1969, en San José de Costa Rica.

⁹ Actualmente, con relación al “*honor*”, el Código Penal Federal vigente en México, contiene derogados todos los artículos del Título Vigésimo titulado *Delitos contra el Honor*; mientras que la Constitución mexicana, sin definir lo que es el honor, solo lo reconoce para la patria (art. 31), y lo relaciona con la honorabilidad que deberán poseer ciertos funcionarios públicos (arts. 95, 100, 116 y 122) como los Ministros de la Corte, los miembros del Consejo de la Judicatura Federal, así como Magistrados y Jueces de los Poderes Judiciales locales.

2.2 Derechos de tercera generación: mención a la protección de datos personales.

En cuanto a la tercera generación, Pérez Luño (2006: 28) expresa que “la estrategia reivindicatoria de los derechos humanos se presenta hoy con rasgos inequívocamente novedosos al polarizarse en torno a temas como el derecho a la paz, los derechos de los consumidores, los derechos en la esfera de las biotecnologías y respecto a la manipulación genética, el derecho a la calidad de vida o a la libertad informática. Así, se abre paso, con creciente intensidad, la convicción de que nos encontramos ante una *tercera generación* de derechos humanos que complementa a las dos anteriores, que se refieren a las libertades individuales y a los derechos económicos, sociales y culturales. De este modo – dice el autor-, los derechos y libertades de la tercera generación se presentan como una respuesta al fenómeno de la denominada “contaminación de las libertades” (*liberties’ pollution*), término con el que alguno sectores de la teoría social anglosajona aluden a la erosión y degeneración que aqueja a los derechos fundamentales ante determinados usos de las nuevas tecnologías”¹⁰.

Los derechos pertenecientes a esta generación son variados, y más aún por la importancia que cada autor les atribuye, según las necesidades sociales. Para Pérez Luño (2006: 29-33) dentro de los derechos de tercera generación más representativos y consolidados, aunque no los únicos, tenemos: la paz (por el desarrollo tecnológico de la industria bélica), la calidad de vida (las cuestiones ecológicas) y la libertad informática (por los bancos de datos). Entre el primero y el segundo se encuentra un nexo por los riesgos de contaminación que conlleva la energía nuclear y las tecnologías radioactivas. Para Rodríguez Palop (2002: 93-94) el catálogo de los derechos de ésta generación estaría configurado por el derecho al medio ambiente, el desarrollo, a la paz, a la autodeterminación de los pueblos y al patrimonio común de la humanidad. Estos derechos surgen en una etapa histórica determinada en Europa occidental y Estados Unidos tras la

¹⁰ Para el autor la revolución tecnológica ha redimensionado las relaciones del hombre con los demás hombres, las relaciones entre el hombre y la naturaleza, así como a las relaciones del ser humano con su contexto o marco cultural o de convivencia. Lo anterior, lo lleva a destacar la importancia de estas mutaciones conductuales, en la constante incidencia de ellas en la esfera de los derechos humanos.

segunda guerra mundial. Durante los años posteriores a 1945, especialmente en la década de los sesenta-setenta surgieron necesidades especiales de los países integrantes del mundo desarrollado, como los derechos propios de la sociedad tecnológica que surgía¹¹.

En esta clasificación, entre otros, se encuentran derechos muy diversificados, tales como: las garantías frente a la manipulación genética, el derecho a morir con dignidad, el derecho al disfrute del patrimonio histórico y cultural de la humanidad, el derecho de los pueblos al desarrollo, el derecho al cambio de sexo, o a la reivindicación de los colectivos feministas de un derecho al aborto libre y gratuito (Pérez Luño, 2006: 33).

Como se ha visto, a través de los comentarios a la clasificación de los derechos humanos en generaciones, no se discute que el derecho a la protección de datos personales sea un derecho propio de última generación. Este se encuentra dentro del catálogo de la tercera generación, dado que se configura en la década de los 70's y a colación del auge de las nuevas tecnologías, y en particular de la informática, la cual avanza cada día a pasos agigantados¹².

¹¹ Rodríguez Palop sitúa estos derechos dentro de la *cuarta generación*. La autora defiende la tesis de la existencia de cuatro generaciones, pues para ella es posible su existencia tanto desde un punto de vista estrictamente histórico como analítico. “Los derechos de cuarta generación, al revelar la existencia de vínculos comunes y necesidades generalizables, y descubrir que la interdependencia global, en orden a la protección de ciertos bienes colectivos, resulta ya inevitable, han reforzado la idea de la solidaridad y se han elevado como una instancia crítica (aunque no destructiva) frente a una filosofía estrictamente individualista. En este sentido se ha dicho que el desafío universal que para la especie humana representan los desastres ecológico, bélico y alimentario, ha de ser abordado desde una razón práctica que consiga dar respuestas universales mediante normas intersubjetivamente válidas independientemente de la existencia de diferentes concepciones morales. Esto no significa incurrir en una indeseable eliminación de las diferencias (aunque si excluye la posición del relativismo moral extremo, no tiene inconveniente en aceptar el pluralismo moral), ni tampoco recurrir a tesis comunitaristas, sino sólo señalar que la autonomía individual se halla inescindiblemente unida a la autonomía pública y que la separación entre intereses individuales y colectivos no puede ser tajante, ni tampoco obedecer a un intento de anteponer en todo caso los primeros a los segundos” (Rodríguez Palop, 2002: 266). Los derechos de ésta generación se han reforzado la idea de solidaridad o cooperación. Puy (1985c: 25) define el *derecho de cooperación* como “el derecho fundamental que tiene todo ser humano, ininterferida (sic) e indiscriminadamente, (1º) a organizar o promover actividades concretas de coproducción solidaria; (2º) y a participar o enrolarse en las ya organizadas; (3º) de carácter local, nacional o internacional que sean unas y otras; (4º) y todo ello (a) con el espíritu y formalidades jurídicas del cooperativismo, el mutualismo o el colaboralismo (sic), (b) y con el objeto o materialidad crematística de hacer efectiva la solidaridad económica especialmente.

¹² Esta idea de derecho de tercera generación es referida también por Cesario (2001: 104) y Flores Dapkevicius (2004: 65).

Así, el individuo demanda una forma eficaz de proteger su derecho a la privacidad (derecho de primera generación), a través de un nuevo derecho que le proteja de intromisiones de terceros y le permita a su vez decidir qué datos proporciona, a quién se los entrega y para qué los utiliza el receptor de los datos. La persona ahora necesita seguridad y protección, frente al posible mal uso que de sus datos personales se haga, por parte de aquellos que sean titulares de ficheros. Estos, hoy en día, dada la era tecnológica en la que vivimos, son en su gran mayoría electrónicos, por lo tanto, son altamente vulnerables de no seguir las medidas de seguridad correspondientes, ya que son de fácil manipulación. De esta forma, y en ésta época, nace un nuevo derecho fundamental, el derecho a la protección de datos personales¹³.

2.3 Consideración a la cuarta generación

Rodríguez Palop (2002: 75-76) dice que desde su punto de vista estrictamente histórico como analítico, es posible hablar de *cuatro generaciones* de derechos humanos. Considera que los derechos civiles y políticos no pueden agruparse en una única categoría, y está de acuerdo con Bobbio, al decir que únicamente desde que se concibió la libertad, no sólo como “no impedimento”, sino positivamente como “autonomía”, se alcanzó una participación cada vez más amplia, difundida y frecuente de los miembros de la comunidad en el poder político (o libertad en el Estado), y por lo tanto, fue en esta segunda fase cuando surgieron los derechos políticos: “La concesión de los derechos políticos ha sido una consecuencia natural de la concesión de los derechos de libertad, porque la única garantía al respeto de los derechos de libertad está en el derecho de controlar el poder” (Bobbio, 1996: 35).

También, hay quien dice que la existencia de una cuarta generación es producto de una nueva etapa –existen tres generaciones, más otra–, que obedece a la necesidad de concebir a la humanidad como una sola familia y que todos sus miembros deben sumar esfuerzos para el bienestar global, y si cualquier integrante de ese cuerpo está adolorido o lesionado, ello inevitablemente

¹³ Este derecho es motivo de nuestra tesis y se verá explicado ampliamente en las páginas de la misma.

redundará en el sufrimiento de todos los demás. Es decir, comprende el derecho a la plena y total integración de la familia humana. Igualdad de derechos sin distinción de nacionalidad, comprende el derecho a formar un Estado y derecho supranacionales (Donaires Sánchez, 2001/2002:195-197)¹⁴.

Otros autores precisan que después de la tercera generación de derechos correspondientes a los de solidaridad, la cuarta atiende a las nuevas formas que cobran los derechos de primera, segunda y tercera generación en el entorno del ciberespacio, es decir, la cuarta generación de los derechos humanos en los que la universalización del acceso a la tecnología, la libertad de expresión en la red y la libre distribución de la información juegan un papel fundamental (Suñé Llinás, 2009: 41-42)¹⁵.

3. Derechos de la personalidad

El derecho a la personalidad en su acepción más *lata*, se refiere al “derecho fundamental que tiene todo ser humano a que los poderes sociales y estatales le permitan desenvolverse libremente en su actuación referente a la adquisición (sic) de un perfil propio, de carácter psicológico, ético y jurídico, que le individualice enérgica y netamente frente al telón de fondo social formado por los

¹⁴ En esta era de Internet, la cibernética y/o lo virtual hay quienes la consideran como la segunda revolución industrial o revolución informática, para mayor abundamiento véase a Pérez Luño (1976: 17-21) y Frosini (1981: 205-207 y 1982: 100-103).

¹⁵ Durante la Segunda Convención Internacional de Derecho Informático, Electrónico y de las comunicaciones, realizado en Oviedo del 30 de marzo al 2 de abril de 2009 y cuyas actas se recogen en el libro que lleva por nombre el título de la Convención, el profesor Emilio Suñé Llinás presenta su propuesta de Declaración de derechos del ciberespacio: texto articulado. La propuesta consta de 22 artículos desarrollados que se titulan: 1. La libertad de información sólo se aplica a la información, 2. Libre e igual acceso a la información, 3. Eliminación de la brecha digital, 4. Accesibilidad de la información, 5. Igualdad de oportunidades en la producción y difusión de información, 6. Equilibrio entre propiedad intelectual y libre flujo de la información, 7. Prohibición de monopolios y oligopolios de información, 8. Derecho a la inviolabilidad de la información, 9. Derecho al Habeas Data, 10. Contenido del Habeas Data, 11. Derechos que limitan el Habeas Data, 12. Derecho al secreto de las comunicaciones, 13. Prohibición de los monopolios de poder en Internet, 14. Protección de menores, 15. Dignidad de la persona, 16. Libertad de trabajo y comercio en el ciberespacio, 17. Protección del patrimonio cultural en el ciberespacio, 18. Derecho ciudadano a la relación telemática con los poderes públicos, 19. Derecho a la autorregulación en un marco de heterorregulación, 20. Garantía institucional de los Derechos Humanos en el ciberespacio, 21. Cláusula de extensión y de progreso, y 22. Cláusula de cierre en evitación de la paradoja de la libertad. Lo que a este estudio interesa es la correspondiente regulación del hábeas data, aunque para mayor abundamiento sobre el tema véase: Suñé Llinás (2009: 39-64).

demás miembros del grupo o grupos sociales a que pertenezca” (Puy, 1985a: 11)¹⁶.

El derecho a la protección de datos personales, es un *derecho de la personalidad*, y como tal es inherente a la persona, con las características propias de estar directamente relacionado con la dignidad humana¹⁷, de no ser susceptible de enajenación y de extinguirse con la muerte. Normalmente el término de “derechos de la personalidad” suele causar confusión y es utilizado como sinónimo de derechos fundamentales, libertades públicas y derechos humanos. Si bien existen similitudes, los derechos de la personalidad difieren de aquellos en lo que respecta a su contenido y protección legal, además de estar comprendidos dentro de las temáticas del Derecho Civil, el cual tiene que ver con los problemas entre particulares. En lo anterior, encontramos una diferencia al contrario de los derechos fundamentales y los derechos humanos, ya que estos tienen que ver con la persona como ciudadano de un Estado, el cual está obligado a respetar y garantizar su debido cumplimiento (Delgado Triana, 2008: 23).

Para Delgado Triana (2008: 26) los *derechos humanos* contienen una gama mayor de derechos que los inherentes a la personalidad, los primeros van más allá de los que le son inherentes a la persona, los colectivos, económicos, sociales y culturales también están contenidos en estos. Los derechos a la personalidad contienen menor cantidad de derechos y solo acogen a los

¹⁶ Para Francisco Puy (1985b: 12) los derechos de la personalidad, están reconocidos por los arts. 10.1, 25.2, y 27.2 de la Constitución española al hacer, todos ellos, referencia “al libre desarrollo de la personalidad”. Además nos dice que “la personalidad no es otra cosa, en principio, que el resultado a que llega el ser humano cuando cumple con la misión que le corresponde, ontológicamente, como persona. A saber: la tarea de trazar una curva vital que dibuje un perfil propio, desarrollando libremente las posibilidades brindadas por la ley de la propia naturaleza. Nunca es posible a ningún hombre, obviamente, desenvolver a la perfección y hasta el final todas las disposiciones latentes en su personalidad. Pero por eso mismo responde a la dignidad de la persona humana la tarea de procurar el mayor despliegue, y la más armónica evolución, de su personalidad psicológica y de su personalidad ética. Que por cierto, se debe distinguir entre ambas. Pues a ambas las comprende el derecho a la personalidad, además de a la personalidad jurídica. Y ambas constituyen muy importantes aspectos del mismo” (Puy, 1985b: 20-21).

¹⁷ “El derecho a la dignidad es el derecho fundamental que tiene todo ser humano para mantener y conservar su naturaleza espiritual íntegra, inviolada, consagrada, no degradada, honrada, no infamada, por razón de su rango y valor de ser el hombre el ser supremo entre todos los seres. El derecho a la dignidad es simplemente el macro-derecho fundamental, el súper-derecho humano, el conjunto de los derechos naturales, el derecho marco o categoría lógica que los abarca a todos” (Puy, 1985a: 89). En lo que hace a la materia de protección de datos personales, Campuzano Tome (2000: 55) dice que, en definitiva, debe ser explorada desde el ángulo de los derechos de la persona.

individuales. Los derechos humanos, han surgido a través de generaciones en la historia, y durante la primera, es que los derechos a la personalidad encuentran su sede. “Los derechos humanos regulan las relaciones Individuo-Estado, al ser propios del Derecho Público, mientras que los derechos inherentes a la personalidad se enmarcan generalmente en regular las relaciones individuo-individuo, al pertenecer al Derecho Privado” (Delgado Triana 2008: 26). Aunque en el caso del derecho a la protección de datos personales, no obstante es un derecho oponible a particulares, también lo es frente a vulneraciones hechas por el Estado. Respecto de los derechos humanos, la principal diferencia con los derechos a la personalidad, es que mientras los primeros se mueven en el ámbito del Derecho Internacional Público, los segundos evocan una norma nacional.

El término *derechos fundamentales* «*droits fondamentaux*» -como se ha precisado con anterioridad- aparece en Francia en 1970 con el movimiento político y cultural que condujo a la Declaración de Derechos del Hombre y del Ciudadano de 1789. Propagándose después por Alemania (Peces-Barba Martínez, 1982: 6). Los derechos fundamentales no son más que los derechos humanos recogidos en las leyes supremas de cada país, con un conjunto de garantías reforzadas para lograr su eficaz cumplimiento. Mientras que los derechos inherentes a la personalidad han sido reconocidos expresamente como derechos fundamentales. Es de señalar que ambos términos no coinciden exactamente, pues los textos constitucionales generalmente reconocen como fundamentales una gama de derechos más amplia; así, por ejemplo, el derecho al trabajo, al descanso retribuido, a la salud pública, a la educación y otros derechos socioeconómicos. (Delgado Triana, 2008: 26-27)

El concepto de *libertades públicas* aparece en Francia a finales del siglo XVIII y expresamente es empleado en el art. 9 de la Constitución de 1793, en el cual se proclama que la ley debe proteger la libertad pública e individual contra la opresión de aquellos que gobiernan. Posteriormente en el art. 25 de la Constitución del II Imperio en 1852, se hace del Senado el guardián de las libertades públicas. Este concepto es distante del reducido campo de los derechos de la personalidad, por lo tanto se asemeja más al de derechos fundamentales, es

decir los derechos humanos volcados a un texto constitucional (Pérez Luño, 1999: 35-36).

Existen bienes de la personalidad no contemplados en el campo de las libertades públicas, muchas de estas nada tienen que ver con los derechos de la personalidad y en ocasiones estos derechos pueden entrar en colisión con las libertades públicas, tal es el caso de los derechos al honor, a la intimidad y a la imagen con la libertad de expresión e información. Los derechos privados entre los que se encuentran los derechos de la personalidad en el ámbito moral delimitan una esfera de libre actividad personal más técnica y no son en modo alguno asimilables a los demás derechos, dado que normalmente no obligan al Estado, siendo susceptibles de crear deberes jurídicos respecto a otras personas privadas. Respecto al honor, intimidad y propia imagen se predica atinadamente la existencia de derechos inherentes a la personalidad (Delgado Triana 2008: 28-29).

El Tribunal Constitucional español en su Sentencia 231/1988, refiere que los derechos fundamentales vinculados a la propia personalidad (derechos de la personalidad), son los derivados sin duda de la dignidad humana¹⁸, que implican la existencia de un ámbito propio y reservado, frente a la acción y conocimiento de los demás, lo que es necesario para mantener un estándar mínimo de calidad de vida. Se muestran esos derechos como personalísimos y ligados a la misma existencia del individuo. Antes se señalaba que estos derechos de la personalidad eran exigibles en la vía civil, por lo que una vez fallecido el titular de los mismos y extinguida su personalidad, lógicamente desaparece también el mismo objeto de la protección constitucional, que está encaminada a garantizar, un ámbito vital reservado, que con la muerte deviene inexistente¹⁹.

¹⁸ Todo ser humano, sea cual sea, posee una dignidad propia, inalienable, en el sentido inequívoco que Kant le dio a este término: aquello que está por encima de cualquier precio y que no admite equivalente alguno, pues no tiene un valor relativo sino absoluto (De Koninck, 2006: 11). Para Landa (2002: 113), la dignidad humana constituye una manifestación del valor de la persona humana y de su libre desarrollo social, este concepto se asienta en un sistema de valores democráticos propios de la posición humanista que adoptó la cultura universal luego del holocausto de la Segunda Guerra Mundial.

¹⁹ En este caso, el Tribunal no podía pronunciarse sobre aquellas cuestiones que, por el fallecimiento del afectado, carecían ya de dimensión constitucional; concretamente, sobre la explotación comercial de la imagen de don Francisco Rivera en el ejercicio de su actividad

Al tratarse de derechos como la intimidad personal y familiar, honor, propia imagen, protección de datos personales, etc., es correcto decir que forman parte de los derechos inherentes a la personalidad. La noción de estos, se reduce a los bienes inseparables de la condición humana, que permiten al hombre el goce de su dignidad y se desarrollan en el campo de las relaciones sociales.

El Tribunal Constitucional Federal de Alemania, en la Sentencia sobre la investigación online en el marco de la lucha antiterrorista²⁰, también se ha pronunciado a favor del derecho al libre desarrollo de la personalidad, cuando dice que este preserva la esfera personal del particular vetando el acceso del Estado a su sistema informático. Si la integridad del sistema informático es puesta en peligro y se permite que terceros accedan a sus funciones, prestaciones y contenidos se produce una injerencia en los derechos fundamentales. Se trate de datos almacenados o archivos temporales, si el sistema se puede considerar propio está protegido por el derecho a la integridad de los sistemas informáticos. En consecuencia, la integridad del sistema informático de un particular es un derecho fundamental derivado del derecho al libre desarrollo de la personalidad (González Pascual, 2009: 949).

profesional. En este aspecto, el «derecho a la imagen» que se invocaba (y al que la demandante concedía especial relevancia) era, en realidad, el derecho a disponer de la imagen de una persona desaparecida y de su eventual explotación económica, protegible, según la Ley 1/1982 en vías civiles, y susceptible de poseer un contenido patrimonial, pero derecho que no podía ser objeto de tutela en vía de amparo, ya que, una vez fallecido el titular de ese bien de la personalidad, no existe ya un ámbito vital que proteger en cuanto verdadero objeto del derecho fundamental aun cuando pudieran pervivir sus efectos patrimoniales (STC 231/1988, de 2 de diciembre, FJ 3).

²⁰ BVerfG, 1 BvR 370/07 vom 27.2.2008. La Ley del *Land Nordrhein-Westfalen* de defensa de la Constitución, de 20 de diciembre del 2006, permitía al Defensor de la Constitución, observar y realizar descubrimientos en Internet, y acceder a sistemas informáticos. La primera medida implicaba el acceso a los contenidos en Internet usando, por ejemplo, Web-Browsers, o participando en chat, o páginas Web poco accesibles, incluso gracias a passwords facilitados por algún informador que dieran acceso a direcciones de correo electrónico o páginas Web protegidas. Aunque en este caso, el derecho implicado es el secreto de las comunicaciones, éste no protege la confianza en un extraño. Los poderes públicos no pueden obtener el password de los particulares sin su autorización y acceder a su mail o a chats privados, pero pueden participar en chats de acceso libre. Ahora bien, la ley no había tenido en cuenta la importancia de los derechos en conflicto, ya que permitía acceder a contenidos sensibles, incluso de terceros no implicados. La segunda medida consistía en la infiltración en sistemas informáticos empleando fallos en la seguridad o instalando programas que permitían observar la utilización del sistema e, incluso, dirigirlo. Sin embargo, los ordenadores son centrales no sólo en nuestro trabajo sino también en nuestras actividades de esparcimiento. La infiltración de un programa espía va mucho más allá del ámbito protegido por el secreto de las comunicaciones, porque permite acceder al empleo estrictamente personal del ordenador, al contenido de múltiples datos e, incluso, al comportamiento en la propia vivienda (González Pascual, 2009: 949).

De lo anterior, se pueden deducir dos cosas, la primera, es que para proteger el desarrollo de la personalidad (que se ejercita a través de los derechos de la personalidad) hay que garantizar la integridad del sistema informático de un individuo; y segundo, que esta integridad es un derecho fundamental derivado. Es interesante, como el mundo de Internet, conduce a la sociedad a la creación de nuevos derechos de acuño jurisprudencial.

4. Regulación normativa internacional de la vida privada

El antecedente del derecho a la protección de datos personales se encuentra en la evolución y desarrollo del derecho a la privacidad, y esto se refleja en la regulación normativa internacional, a través de la Declaración Universal de los Derechos Humanos y el Pacto de San José; así como en la normatividad europea, como el Convenio Europeo de Derechos Humanos, la Directiva 95/46/CE y la Carta de los Derechos Fundamentales de la Unión Europea²¹.

El derecho a la vida privada es de suma importancia para el adecuado desenvolvimiento de la persona, y a través del tiempo ha sido protegido por diferentes instrumentos internacionales como²²:

- La Declaración Universal de Derechos Humanos.
- La Carta Internacional de Derechos Humanos, en su Pacto Internacional de Derechos Civiles y Políticos.
- La Convención Americana de Derechos Humanos.

²¹ Para mayor amplitud del tema sobre la normativa internacional y comunitaria es interesante el trabajo de Dávila Rodríguez (2004: 745-758).

²² El legislador mexicano, en el preámbulo de los Lineamientos de Protección de Datos Personales, de 27 de julio de 2005 (DOF 30/09/2005), reconoce que a nivel internacional se configura la existencia del derecho a la privacidad, de la siguiente forma: “ninguna persona puede ser objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o a su reputación, gozando del derecho a la protección de la ley contra las injerencias o ataques”, estableciéndose así en instrumentos internacionales, los cuales por virtud del art. 133 Constitucional constituyen Ley Suprema de la Unión, como la Declaración Universal de los Derechos Humanos (art. 12); el Pacto Internacional de Derechos Civiles y Políticos (art. 17); la Declaración Americana de los Derechos y Deberes del Hombre (art. V); la Convención Americana sobre Derechos Humanos (art. 11), y la Convención sobre los Derechos del Niño (art. 16).

- El Convenio Europeo de Derechos Humanos.
- La Carta de los Derechos Fundamentales de la Unión Europea.

En las siguientes páginas, se verá cómo se ha protegido internacionalmente el derecho a la privacidad, y como ha sido su desarrollo para arrojar el nuevo derecho fundamental a la protección de datos personales. Dentro de la referencia que se hace de cada uno de los instrumentos, se puntualizan los dispositivos que son de interés para este tema, y para una mayor comprensión del lector he considerado importante hacer una breve descripción de los antecedentes, fines, objetivos y contenido de cada uno.

4.1 Declaración Universal de los Derechos Humanos.

La Declaración Universal de Derechos Humanos, es un instrumento por demás estudiado en estos 60 años transcurridos desde su proclamación. Con sus 30 artículos consagra los derechos de la persona, para protegerla de arbitrariedades y violaciones que históricamente el individuo había venido padeciendo. Bobbio (1991: 64) dice que ésta representa la manifestación de la única prueba por la que un sistema de valores puede ser considerado humanamente fundado y, por tanto, reconocido, esta prueba es el consenso general acerca de su validez.

Una Declaración es un código moral significativo, pero no es una ley, y la transición de ésta a instrumentos normativos vinculantes se retrasó, ya que el Convenio Internacional sobre Derechos Económicos, Sociales y Culturales y el Convenio Internacional sobre Derechos Civiles y Políticos no fueron adoptados hasta 1966. Así, la Declaración de 1948, junto a los dos Acuerdos Internacionales en 1966, han sido denominados “el régimen internacional de los derechos humanos”, que deben de ser considerados los mayores y más importantes instrumentos para salvaguardar estos derechos (Verhellen, 2002: 63).

a) Antecedentes

Célebre es el día 10 de diciembre de 1948, en el que la Asamblea General de las Naciones Unidas reunida en París, en el Palacio de *Chaillot*, aprobó y

proclamó la Declaración Universal de Derechos Humanos. Cuarenta y ocho países aprobaron la Declaración y ocho países decidieron abstenerse (dos países estaban ausentes en el momento de la votación)²³.

Tras este acto histórico, la Asamblea pidió a todos los países miembros que publicaran el texto de la Declaración y dispusieran que fuera “distribuido, expuesto, leído y comentado en las escuelas y otros establecimientos de enseñanza, sin distinción fundada en la condición política de los países o de los territorios”. Así, hoy en día, dicha declaración sigue siendo citada y estudiada por diferentes disciplinas, principalmente, de las Ciencias Sociales. Ello con la finalidad –como lo proclama la declaración- de que tanto los individuos, como las instituciones, inspirándose constantemente en la Declaración, promuevan el respeto a estos derechos y libertades, y aseguren por medidas progresivas de carácter nacional e internacional su reconocimiento y, aplicación universal y efectiva, tanto entre los pueblos de los Estados miembros como entre los de los territorios colocados bajo su jurisdicción.

La Declaración contiene principalmente el reconocimiento de los derechos inherentes e inalienables de la persona, como el respeto a la paz, justicia, vida, libertad, igualdad, dignidad y educación, entre otros; que han sido ícono para promover el respeto de la persona, en las Constituciones de los diferentes países adheridos a la DUDH, los cuales hoy en día son casi todos del orbe²⁴.

No obstante la confianza en la humanidad y en las instituciones que inspiran la DUDH, la gran mayoría aún duda de que los derechos humanos sean una realidad. Vacilación, por otro lado justificada, dado el alto índice de desigualdad entre los individuos y las naciones. Estas desigualdades sociales, culturales y económicas, conducen inevitablemente a la violación e

²³ Los países que aprobaron la Declaración son: Afganistán, Argentina, Bélgica, Birmania, Bolivia, Brasil, Canadá, Colombia, Costa Rica, Cuba, China, Dinamarca, Ecuador, Egipto, El Salvador, Estados Unidos de América, Etiopía, Filipinas, Francia, Grecia, Guatemala, Haití, India, Irak, Irán, Islandia, Líbano, Liberia, Luxemburgo, México, Nicaragua, Noruega, Nueva Zelandia, Países Bajos, Pakistán, Panamá, Paraguay, Perú, Reino Unido, República Dominicana, Siam, Siria, Suecia, Turquía, Uruguay y Venezuela. Los países que se abstuvieron: Arabia Saudita, Bielorrusia, Checoslovaquia, Polonia, Ucrania, Unión Soviética, Unión Surafricana y Yugoslavia.

²⁴ Actualmente la Organización Nacional de Naciones Unidas está formada por 192 países independientes.

incumplimiento de los derechos consagrados por la Declaración. Sin embargo, la evolución de la humanidad registra esfuerzos recurrentes para lograr un verdadero respeto de los derechos inherentes a la persona.

La Declaración de Independencia desde 1776, reivindicó los derechos de los americanos del norte delante de la corona inglesa²⁵. Posteriormente, la revolución francesa, el 26 de agosto de 1789, proclamó la Declaración de los derechos del hombre y del ciudadano, que ha tenido señalada influencia no solamente en el continente europeo, sino en todo el mundo. Pero, a pesar de dicho documento francés, escrito e intensamente defendido, han acontecido episodios en la historia de la humanidad, que han llevado consigo efectos de gran crueldad. Por ejemplo, el choque el 24 de junio de 1859, entre franceses y austríacos en la Batalla de Solferino, cuyo recuerdo recogió Henry Dunant para auspiciar la fundación de la Cruz Roja Internacional, constituida formalmente en 1863. Después, aconteció la calamidad de la Primera Guerra Mundial (1914-1918). Luego, durante la Segunda Guerra Mundial, el holocausto del nazismo conmovió a todos con los campos de concentración instalados para exterminar a los judíos (Gómez Gómez, 2006: 6). Al finalizar, tan penoso episodio de la Historia Universal, por la crueldad con la que se pueden llegar a tratar los humanos entre sí, las Naciones Unidas encuentran en el sentimiento y coraje de los países el campo dispuesto para pronunciar la Declaración Universal de Derechos Humanos.

En este sentido, los considerandos del preámbulo de la Declaración, advierten que el desconocimiento y el menosprecio de los derechos humanos han originado actos de barbarie ultrajantes para la conciencia de la humanidad; y que se ha proclamado como la aspiración más elevada del hombre, el advenimiento de un mundo en que los seres humanos, liberados del temor y de la miseria, disfruten de la libertad de palabra y de creencias. Y asientan la importancia de que los derechos humanos sean protegidos por un régimen de Derecho, a fin de

²⁵ Declaración de independencia de los Estados Unidos de América (Declaración de *Philadelphia*), aprobada por el Congreso el 4 de julio de 1776. En su preámbulo aparece la característica de la “inalienabilidad” de los derechos humanos, citando lo siguiente: “*sostenemos por evidentes en sí mismas estas verdades, que todos los hombres son creados iguales, que son dotados por su Creador de ciertos derechos inalienables, que entre estos están la vida, la libertad y el derecho a la felicidad*”.

que el hombre no se vea compelido al supremo recurso de la rebelión contra la tiranía y la opresión; así como la promoción del desarrollo de relaciones amistosas entre las naciones.

La Declaración de 1948 supone un impulso de emancipación del hombre, tanto a nivel internacional como a nivel interno, porque supone el principio del fin de la mediación del Estado soberano en las relaciones internacionales del ser humano. Es en este punto, que el hombre es reconocido como sujeto de Derecho Internacional Público; y se transforma, con el incremento de reglas internacionales sobre su protección, en un agente de gran relevancia internacional (Rainer, 1998: 59-60).

b) Objeto y fin

La Asamblea General de Naciones Unidas proclama la Declaración Universal de Derechos Humanos como ideal común por el que todos los pueblos y naciones deben esforzarse, a fin de que tanto los individuos como las instituciones, inspirándose constantemente en ella, promuevan, mediante la enseñanza y la educación, el respeto a estos derechos y libertades, y aseguren, por medidas progresivas de carácter nacional e internacional, su reconocimiento y aplicación universales y efectivos, tanto entre los pueblos de los Estados Miembros como entre los de los territorios colocados bajo su jurisdicción.

c) Contenido

La DUDH en sus 30 artículos protege distintos derechos y libertades sin distinción de raza, color, sexo, idioma, religión, nacionalidad, opinión política, etc.; por ejemplo: el derecho a la vida, libertad, la seguridad de su persona, la prohibición de la esclavitud, la servidumbre y torturas. Asimismo, se protege el derecho al reconocimiento de la personalidad, la igualdad ante la ley, el derecho al recurso efectivo ante los tribunales nacionales, se prohíbe el arresto arbitrario, se tutela el derecho al debido proceso y garantías penales. Contiene además la prohibición de injerencias en la vida privada, familia, domicilio o correspondencia.

Se establece el derecho de las personas a la libre circulación, residencia, entrada y salida del país, el derecho de asilo en otro país, el derecho a una nacionalidad, a no ser privada de ella, así como el de cambiar de nacionalidad. Se protege el derecho a contraer matrimonio y fundar una familia. Refiere el derecho a la propiedad, libertad de pensamiento, religión, expresión y reunión. Establece además, el derecho a participar en el gobierno, así como la voluntad del pueblo como base de la autoridad del poder público, además del derecho al voto universal y secreto, el derecho a la seguridad social de toda persona por ser miembro de la sociedad, así como la satisfacción de los derechos económicos, sociales y culturales. Se protege también el derecho al trabajo igual, al descanso, el disfrute del tiempo libre y de vacaciones periódicas pagadas. Se tutela el derecho a un nivel de vida adecuado para cubrir las necesidades básicas, derecho al seguro en caso de desempleo, enfermedad, invalidez, viudez y vejez; así como los derechos especiales de maternidad e infancia, el trato igual para los hijos nacidos fuera del matrimonio. Además, el derecho a la educación elemental gratuita, se establece que sea obligatoria, y que el acceso a los estudios superiores sea igual para todos, etc.

Los derechos enumerados en la Declaración no son los únicamente posibles, sino sólo aquellos que habían sido configurados en la mente de los redactores de la Declaración después de la tragedia de la Segunda Guerra Mundial, en una época que había tenido comienzo con la Revolución Francesa y había llegado hasta la Revolución Soviética (Bobbio, 1991: 71). En este sentido, es que hoy en día aparecen derechos nuevos, que son creados en función de las necesidades de la sociedad actual, tal es el caso de la protección de datos personales o los derechos medio ambientales.

d) Funciones de la Declaración de 1948

La Declaración, aunque no sea una resolución obligatoria, cumplió una importante *función de orientación*, porque en su momento recoge las opiniones de los diferentes países que conformaban la Organización de Naciones Unidas. De este modo, el contenido de dicho instrumento, contenía una nueva orientación para los países miembros en el respeto de los derechos humanos, y la censura a

las violaciones que de estos se hiciera. Así, los países adheridos a la Declaración adquirieron la obligación de reconocer y tutelar los derechos humanos dentro de su legislación interna, para ajustarse jurídicamente a aquella por la lucha a favor de tales prerrogativas.

En su aspecto internacional la función de orientación, es doble: funcional y material. La *funcional* consiste en que la tarea de respetar los derechos humanos pasa a ser un cometido internacional garantizado por la comunidad de naciones; ésta, es una característica fundamental de los tratados ratificados por los países firmantes, por el que se obligan recíprocamente a la protección de los derechos en beneficio de las personas, de las naciones y de las relaciones con otros Estados. La *material* se refiere a que los ordenamientos nacionales que no han adoptado aún un sistema de protección adecuado de esos derechos deben seguir la línea directriz de la Declaración (Rainer, 1998: 60-61).

La función material es cardinal para cualquier tratado, cuya finalidad sea la protección de algún derecho, porque no basta la característica *funcional* de reconocimiento, se necesita además, la implementación de un órgano eficaz que vele por la protección, fomento y legislación de los derechos. Que garantice, principalmente, la eficaz aplicación de las normas protectoras de tales prerrogativas, así como la sanción que devenga de las violaciones a dichas normas. Por ello, se advierte la necesidad de un órgano o institución especial que atienda las necesidades propias de la función material en comento.

La existencia de un órgano protector de los derechos humanos, es hoy en día una realidad en muchos países. En México existe, sin embargo, –y no obstante el esfuerzo de la Comisión Nacional de Derechos Humanos y las comisiones estatales- sus resoluciones no llegan a ser un instrumento eficaz para la protección de los derechos, toda vez que se quedan como meras recomendaciones, es decir, directrices de actuación y carentes de coercibilidad efectiva por parte de la Comisión hacia los organismos públicos.

A la idea de guía u orientación, se encuentra íntimamente ligada otra paralela, la *función de impulso*. La *orientación* es la dirección que habrán de seguir los diferentes países dentro de sus ordenamientos internos, ajustándose al

Tratado, para la debida protección de los derechos humanos. La Declaración también implica una obligación –no coercitiva- de ajustar sus ordenamientos internos a la normativa internacional, y así promover en la nación como entre los ciudadanos el respeto idóneo de los derechos humanos. Por tanto, la función de *impulso* implica un acuerdo de los países y una obligación no coercitiva para estos de legislar internamente acorde a la Declaración.

La cooperación internacional entre Estados, debe de revestirse de una característica fundamental, para que dicha cooperación, así como las relaciones internacionales, se desarrollen en un espacio de armonía y confianza. Tal característica estriba en el hecho de que entre los Estados exista una debida tutela y reconocimiento de DDHH. Los avances existentes en esta materia, se encuentran principalmente en los países europeos. Por otro lado, con una visión algo conformista, si se observan algunos países latinoamericanos, es comprensible que el respeto de los DDHH no sea coercitivo (porque la coercibilidad implicaría la existencia de una sanción, que de haberla, nos conduciría al resultado de su aplicación masiva), y que si bien no se protegen en su totalidad los derechos consagrados en la DUDH, aquellos que se logren proteger, ya constituye un avance para la Declaración.

Si bien la última idea pareciera impregnada de un alto grado de conformismo y de justificación, responde a una realidad –difícil de negar- existente en muchos países, y que lejos del pesimismo, atiende a un optimismo de que las grandes cosas se construyen por el cúmulo de varias pequeñas, avanzando a paso firme.

e) Efectos de la Declaración Universal de Derechos Humanos

La DUDH envuelve en si misma distintos efectos, los cuales son: a) emancipatorio, b) integrativo, c) constituyente, y d) formativo cultural. Estos, hacen de la Declaración un documento único, de importancia y aplicación universal, por el compromiso adquirido de los países que la han ratificado.

1. Efecto emancipatorio

La idea del efecto emancipatorio se refiere a la internacionalización que se hace de los derechos humanos, los cuales existían en diferente medida dentro de las legislaciones nacionales, transmutando a ser reconocidos y ampliados internacionalmente por los Estados miembros de Naciones Unidas. De esta forma, el individuo no solo cuenta con un garante nacional, sino también con uno internacional.

En esta transformación de la idea de protección del hombre a nivel internacional se muestra un efecto importante de emancipación del individuo, ya que dicha internacionalización significa una universalización de los Derechos Humanos, convirtiéndose en la primera materia concerniente a una relación entre el individuo y el Estado, es decir, una materia de dimensión interna, que se internacionaliza y universaliza (Rainer, 1998: 63-64).

Con relación a la idea anterior, existe una rama del Derecho Internacional (DI), creada por la doctrina, que es el Derecho Internacional de los Derechos Humanos (DIDH), la cual implica como primera idea, que los derechos humanos son materia del DI. Y que por tanto, el DIDH es diferente del Derecho Internacional Común (DIC), ya que este último tiene por objeto las relaciones entre los Estados y otras personas de Derecho Internacional (como los organismos internacionales). En cambio en el DIDH lo que se regula no son las relaciones anteriores, sino derechos entre Estados (que aparecen siempre como el sujeto pasivo, es decir como parte obligada) y seres humanos (son por excelencia el sujeto activo, o sea, los titulares de los derechos) que no aparecen como sujetos típicos de ese Derecho Internacional (Piza y Trejos, 1989: 61-62).

2. Efecto integrativo

La universalización de la garantía de los derechos humanos, a que anteriormente se hizo referencia durante el análisis del efecto emancipatorio, hace común un único concepto de la dignidad, la libertad y la autonomía del hombre destinado a la constitución de los derechos básicos de la persona (Rainer, 1998: 64).

La influencia de los instrumentos internacionales sobre los ordenamientos internos es más intensa a nivel regional que en el universal, en la que se producen también efectos horizontales y verticales aunque con menor intensidad que en los ámbitos regionales; ya que se puede constatar fácilmente un efecto integrativo que resulta de una determinada Convención regional de derechos humanos, el efecto horizontal y vertical. La *Convención* constituye un texto de garantías iguales para un determinado número de Estados, lo que produce una armonización de los valores fundamentales en toda la región (efecto *horizontal*). Al mismo tiempo la Convención, por su influencia sobre el ordenamiento interno, origina una armonización entre Convención internacional y derecho interno (efecto *vertical*). Los efectos verticales suponen por sí mismos un efecto integrativo horizontal, a nivel interno entre los Estados cuyos ordenamientos normalmente son independientes; esa separación se ve disminuida por dicha integración de valores (Rainer, 1998: 64-65). Un ejemplo de lo anterior, lo encontramos al interior de un Estado Federal en relación con sus entidades federativas –como el caso mexicano–, en donde cada una de éstas cuenta con su propia Constitución y, al encontrarse subordinadas a la Constitución Federal, habrán necesariamente de situarse en el mismo contexto de ésta en lo relativo a las disposiciones protectoras de los derechos humanos.

3. Efecto constituyente

Actualmente, en muchos Estados las garantías consagradas en la DUDH, han adquirido la importancia necesaria para considerarse de nivel constitucional. Tal jerarquía, se encuentra plasmada en las Constituciones de países como España, Argentina, Rumanía y Portugal, entre otros; que refieren la Declaración en el cuerpo normativo de sus textos constitucionales.

Este efecto es muy significativo, dado que la ONU no es propiamente un Estado, ni sus Tratados una Constitución. Sin embargo, dentro de la regulación jurídica internacional, las Convenciones protectoras de los derechos humanos constituyen una especie de desarrollo del Derecho Constitucional. Esto se ve reflejado, por la voluntad de los Estados en reconocer un poder de orden

supranacional, por ello, es que se pudiera comparar –muy limitadamente- a la ONU con un Estado (Rainer, 1998: 65).

En el Estado, la Constitución se basa en el reconocimiento de valores comunes que son el marco de la acción política, siendo las principales características de una Constitución el apartado referente al reconocimiento y protección de los derechos humanos, y aquel relativo a las disposiciones que contienen la organización política, administrativa, territorial y jurídica del mismo. A nivel universal, las garantías de los derechos humanos presentan, en sí mismas, la tendencia a consolidarse y a desarrollarse por la interpretación y por su aplicación en la práctica, aunque esta última es un elemento problemático en un ordenamiento compuesto de Estados soberanos con relaciones de coordinación (Rainer, 1998: 66). En donde dicha coordinación, entre países, a veces se ve afectada por la diversidad cultural e histórica, y por la realidad socioeconómica de cada uno, no obstante estas diferencias, las garantías de los derechos humanos, se han ido homogenizando, si bien no en la práctica del modo de ejecución, si en su aspecto formal, ya que cada Estado cuenta con una estructura institucional propia.

Este efecto, es de considerarse el más importante, porque, ya sea de manera directa, en donde los derechos pasen a formar parte de la legislación interna, o bien, de modo vinculante con la Constitución en relación a la DUDH; bien sea de un modo o de otro, los derechos son efectivos para las personas. La constitucionalización de los derechos humanos, hace posible la creación de un organismo encargado de velar por la protección de los derechos de la persona. Es de señalar que de todos los efectos de la Declaración, el más importante es precisamente el de su constitucionalización, ya que de lo contrario el ciudadano se encuentra ante una evidente inseguridad jurídica.

4. Efecto formativo cultural

La comunicación, a través de sus distintos medios, ha sido por excelencia la forma de promover cualquier cosa o actividad. Por tanto, juega un papel de suma importancia para la divulgación de aquello que los Estados a nivel nacional e internacional llevan a cabo. La Declaración, como política de nivel

internacional, ha sido ampliamente difundida entre las personas alrededor del orbe, por ser los derechos más esenciales del ser humano. Por tal motivo, ha sido vital que se dé a conocer más allá del simple aparato gubernamental ejecutor.

El impulso dado por la Declaración de 1948, inició a nivel universal, un proceso irreversible en la promoción del bienestar humano. Ya que, tras la Segunda Guerra Mundial, en los ordenamientos internos y en particular de los Estados europeos el antropocentrismo es una característica particular que los distingue, de aquellos que fueron elaborados en otros periodos (Rainer, 1998: 66). Este desarrollo parece tan fundamental que forma parte de las bases contemporáneas de la cultura. Por ello, la Declaración de 1948 constituye, sin lugar a dudas, un hito en el progreso cultural porque logra recopilar los derechos universales –y no particulares de cada Estado- para lograr precisamente ese bienestar humano.

f) Artículo relacionado

La Declaración Universal de los Derechos Humanos, en su art. 2 del apartado correspondiente a los derechos civiles y políticos, establece que todo individuo tiene derecho a la vida, a la libertad y a la seguridad de su persona. Seguridad que se habrá de entender en su sentido más amplio, considerando así que las injerencias a la vida privada de una persona pueden causar un gravamen a la seguridad física y mental de un individuo.

El art. 8 de dicho ordenamiento, establece que toda persona tiene derecho a un recurso efectivo ante los tribunales nacionales competentes, que la amparen contra actos que violen sus derechos fundamentales reconocidos por la Constitución o por la ley. Este dispositivo pone de manifiesto el derecho de toda persona a contar con un instrumento de protección brindado por el Estado para garantizar sus derechos.

En el caso mexicano, el derecho a la privacidad y específicamente el relativo a la protección de datos personales, se encuentra en vías de desarrollo y fortalecimiento, aunque el primero más avanzado que el segundo. Lo anterior, toda vez que no es hasta el año 2010 que se publica en el Diario Oficial de la

Federación la Ley Federal de Protección de Datos Personales en México, la cual ha entrado en vigor un año después de su publicación²⁶.

Específicamente el art. 12 DUDH, establece que nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o a su reputación. Además agrega que toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques, lo que se relaciona directamente con el art. 8 DUDH, antes referido.

Los datos personales todo el tiempo han existido, y han sido protegidos por la persona al reservarse, a veces celosamente, cierta información para sí, y su grupo familiar; no obstante ello, en la primera mitad del siglo XX, estos no constituían una preocupación fundamental en la vida cotidiana, al no existir la cantidad de avances tecnológicos con los que hoy se interactúan diariamente, situación que propicia la vulnerabilidad del individuo en su vida privada

Las nuevas tecnologías, constantemente enfrentan al individuo con una nueva realidad, a la que difícilmente se puede dar marcha atrás. Por ello, al Derecho no le queda otro camino, que el regular jurídicamente los nuevos escenarios que se producen, con la realidad que ofrecen, tanto en lo que hace a los efectos positivos, como los negativos, por ejemplo, en las últimas décadas se ha visto la regulación del comercio y la firma electrónica.

México cuenta con mecanismos de protección de datos personales con relación a salvaguardar la vida privada, y entre ellos están los que provee el Instituto Federal de Acceso a la Información Pública, al que se le reconoce el esfuerzo por su trabajo, pero también es de señalar la tibieza del legislador mexicano al no haber aprobado las primeras propuestas de ley de protección de datos personales presentadas desde 2001²⁷. Asimismo, es de reconocerse el avance dado en la materia producto de las últimas reformas producidas a partir el

²⁶ Esto se ha desarrollado más detalladamente el capítulo correspondiente a la protección de datos personales en México.

²⁷ El 14 de febrero de 2001, el Senador Antonio García Torres presentó el primer proyecto de Ley de protección de datos personales, sin embargo no prosperó.

año 2007, que inicia con la del artículo 6 de la Constitución Política de los Estados Unidos Mexicanos, que se tratará con posterioridad²⁸.

Hasta 2010, cuando aún no existía la Ley Federal de Protección de Datos Personales, las previsiones a este derecho sólo se encontraban en lo dispuesto por un capítulo de apenas siete artículos dentro de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental, misma que en realidad no brindaba una total seguridad jurídica a las personas en relación con el tema.

4.2 Carta Internacional de los Derechos Humanos: referencia al Pacto Internacional sobre Derechos Civiles y Políticos.

La Carta Internacional de los Derechos Humanos (CIDH), constituye el principal documento que reúne los instrumentos jurídicos internacionales más importantes destinados al reconocimiento y protección de los derechos humanos, y se compone de:

- La Declaración Universal de los Derechos Humanos (10/12/1948)
- El Pacto Internacional de Derechos Civiles y Políticos (23/03/1976).
- El Pacto Internacional de Derechos Económicos, Sociales y Culturales (03/01/ 1976).
- El Protocolo Facultativo del Pacto Internacional de Derechos Civiles y Políticos (23/03/1976).
- El Segundo Protocolo Facultativo del Pacto Internacional de Derechos Civiles y Políticos, destinado a abolir la pena de muerte (15/12/1989).

a) Antecedentes

Comenzadas las actividades de Naciones Unidas, tres años después la Asamblea General estableció la piedra angular de la legislación contemporánea en materia de derechos humanos la “Declaración Universal de Derechos Humanos”, aprobada el 10 de diciembre de 1948, con la finalidad de ser el "ideal común por el que todos los pueblos deben esforzarse". En este documento se detallan -como se ha mencionado con anterioridad- los derechos fundamentales

²⁸ Reformas de los artículos 6, 16 y 73 de la Constitución mexicana.

civiles, culturales, económicos, políticos y sociales, que deben disfrutar todas las personas de todos los países²⁹. Por ello, el 10 de diciembre es conmemorado en todo el mundo como el día internacional de los derechos humanos.

Se considera que las disposiciones de la Declaración Universal de Derechos Humanos tienen carácter de Derecho Internacional consuetudinario, dado que están ampliamente aceptadas y se utilizan como pautas de conducta a seguir por los Estados. Actualmente algunos de los países que han obtenido recientemente su libertad, citan la Declaración en su ordenamiento de mayor jerarquía, tal es el caso de las constituciones de España, Argentina, Rumania, Portugal, Ruanda y Cambodia, entre otras³⁰.

b) Objeto y fin

La Carta Internacional de los Derechos Humanos (CIDH) persigue el mismo fin que la Declaración Universal de Derechos Humanos, que es precisamente en la que se han inspirado la serie de convenios internacionales que han surgido con posterioridad. Por ello, las naciones siguen un objetivo común en la protección de los derechos humanos sin importar la raza, la nacionalidad, el sexo, la religión, las ideas políticas, etc. Así la CIDH, ha redefiniendo y desarrollado los derechos tutelados por la DUDH, a través de los pactos y protocolos subsecuentes.

c) Contenido

Dentro de los acuerdos vinculantes sobre derechos humanos que se negocian bajo los auspicios de las Naciones Unidas, aquellos que tienen un alcance más amplio son los dos Pactos Internacionales: uno de Derechos Económicos, Sociales y Culturales y otro de Derechos Civiles y Políticos. Esos acuerdos, aprobados por la Asamblea General en 1966, desarrollan la Declaración Universal, ya que plasman en obligaciones jurídicas los derechos que figuran en

²⁹ <http://www.cinu.org.mx/onu/documentos/ciddh.htm#carta> (consulta: 09/11/2012).

³⁰ Estas son las fechas de las Constituciones y el artículo que refiere la Declaración Universal de Derechos Humanos: España (6/12/1978, art. 10), Argentina (22/08/1994, art. 75.22), Rumania (8/12/1991, art. 20.1), Portugal (2/04/1976, art. 16.2), Ruanda (30/05/1991, en su preámbulo) y Cambodia (21/09/1993, art. 31).

ella y establecen órganos para vigilar el cumplimiento por los Estados firmantes. La mayoría de los países son partes en los Pactos.

La Declaración Universal junto con los dos Pactos Internacionales de Derechos Humanos y sus Protocolos facultativos, constituyen la Carta Internacional de los Derechos Humanos, y ésta última se compone del texto de los siguientes documentos:

- La Declaración Universal de los Derechos Humanos (10 de diciembre de 1948).
- El Pacto Internacional de Derechos Civiles y Políticos (23 de marzo de 1976).
- El Pacto Internacional de Derechos Económicos, Sociales y Culturales (3 de enero de 1976).
- El Protocolo Facultativo del Pacto Internacional de Derechos Civiles y Políticos (23 de marzo de 1976).
- El Segundo Protocolo Facultativo del Pacto Internacional de Derechos Civiles y Políticos, destinado a abolir la pena de muerte (15 de diciembre de 1989).

Los artículos relativos al derecho de privacidad y de protección de datos personales, dentro de los instrumentos de Derecho Internacional, se señalan en la Declaración Universal –referida con anterioridad- y el Pacto Internacional de los Derechos Civiles y Políticos.

Pacto Internacional sobre Derechos Civiles y Políticos.

La CIDH recoge los derechos civiles y políticos el 23 de marzo de 1976, con el fin de garantizar el respeto a la dignidad humana, igualdad, vida, seguridad jurídica y libertad de las personas. Un rasgo novedoso de este instrumento jurídico internacional fue el establecimiento de un órgano de expertos para supervisar su aplicación, el Comité de Derechos Humanos, cuya composición se regula en el apartado IV del Pacto.

a) Antecedentes

El Pacto Internacional de Derechos Civiles y Políticos fue aprobado por la Asamblea General de la ONU, mediante la resolución 2220 A (XXI), del 16 de diciembre de 1966. Este Pacto entró en vigor el 23 de marzo de 1976 al haberlo ratificado o haberse adherido a él 35 Estado. El mismo día 12 Estados ratificaron el Protocolo Facultativo, que en consecuencia también entro en vigor. Posteriormente, en enero de 2003, 149 Estados habían ratificado el Pacto o se habían adherido a él³¹.

La Carta se integra de dos pactos, el de los derechos civiles y políticos, y el relativo a los derechos económicos, sociales y culturales (1966). La existencia de ambos se justifica ampliamente dada la diversa naturaleza de cada uno. Las disposiciones del Pacto de Derechos Civiles y Políticos que define libertades de primer orden, son disposiciones *inmediatamente aplicables* según obra en el art. 2, por el que se establece que los Estados parte del pacto se comprometen a adoptar las medidas correspondientes a través de los procedimientos constitucionales de los propios países, a fin de garantizar el cumplimiento y respeto de los derechos que ahí se establecen. Mientras que tratándose de los derechos económicos, sociales y culturales del segundo Pacto, los Estados se comprometen a actuar en orden de asegurar “*progresivamente*” el pleno ejercicio de los derechos ahí reconocidos, a través de los medios apropiados refiriendo que incluyendo la adopción de medidas legislativas, para lograr la plena efectividad de los derechos ahí reconocidos, según lo refiere el artículo 2 del mismo pacto.

b) Objeto y fin

Los dos pactos de la CIDH, si bien protegen derechos de diferente índole, recogen el mismo espíritu en su preámbulo, el cual consiste en que la libertad, la justicia y la paz en el mundo tienen por base el reconocimiento de la dignidad inherente a todos los miembros de la familia humana y de sus derechos iguales e inalienables

³¹<http://www.cinu.org.mx/onu/documentos/pidcp.htm> (consulta: 09/11/2012). México, al depositar su instrumento de adhesión al Pacto el 23 de marzo de 1981, formularía dos declaraciones interpretativas (art. 9, pár. 5, y 18) y dos reservas. La promulgación de este Pacto en México se realizó el 30 de marzo de 1981, y se publicó en el Diario Oficial de la Federación, el 20 de mayo de ese mismo año (Carpizo Mc-Gregor y Gómez-Robledo Verduzco, 2000: 33-34).

Estos pactos se crean con la finalidad de crear las condiciones que permitan a cada persona gozar de sus derechos civiles y políticos liberados del temor y la miseria, para realizar el ideal del ser humano libre, el cual es el disfrute de las libertades civiles y políticas.

c) Contenido

El Pacto se compone de 53 artículos divididos en seis partes, de la siguiente forma:

- *Parte I.* Comprende la libre determinación de los pueblos respecto de su condición y desarrollo político, económico, cultural y social.
- *Parte II.* Establece el compromiso de los Estados parte a garantizar los derechos reconocidos por el pacto, asimismo los compromete a legislar en sus ordenamientos internos para cumplir con aquel. Se establecen los casos, las excepciones y el procedimiento para suspender los derechos pactados, así como la prohibición de restringir o menoscabar tales derechos.
- *Parte III.* Garantiza el derecho a la vida, a la igualdad, regula el procedimiento a la pena de muerte establecida en los países partes del pacto, la prohibición de la tortura, la esclavitud, la servidumbre y el trabajo forzoso. Se establece además el derecho a la libertad y a la seguridad personal, el derecho a un proceso penal, la regulación del régimen penitenciario. También contiene la libertad de salir, entrar y circular libremente por el territorio de un Estado. Se regulan las garantías de seguridad jurídica y del debido proceso, el derecho al reconocimiento de la personalidad jurídica, el *derecho a la vida privada y no injerencias arbitrarias*. Refiere la libertad de pensamiento, conciencia, religión, opinión y expresión. Establece la prohibición de propaganda a favor de la guerra o el racismo. El derecho a la reunión pacífica, de asociación, a la propia vida cultural de las etnias, así como el derecho a contraer matrimonio, garantiza los derechos básicos de los niños, así como el de las personas para votar y ser votados en la participación de la vida política de su país.

- *Parte IV.* Contiene los lineamientos de composición del Comité de Derechos Humanos.
- *Parte V.* Regula la interpretación del pacto.
- *Parte VI.* Comprende la regulación respectiva a la firma y vigencia del pacto.

d) Artículo relacionado

El Pacto Internacional de Derechos Civiles y Políticos, en su artículo 17 protege el derecho a la vida privada, desde la prohibición de las injerencias arbitrarias o ilegales que se hagan a las diferentes esferas de la vida privada del individuo tales como la familia, el domicilio, la correspondencia, la honra y la reputación. Así mismo establece el derecho que tiene toda persona a la protección de la ley contra esas injerencias o esos ataques.

El art. 9.2 de este pacto, señala que toda persona detenida será informada, en el momento de su detención, de las razones de la misma, y notificada, sin demora, de la acusación formulada contra ella. Si bien este precepto contiene elementos de seguridad jurídica, también es importante destacar que la información en dicha acusación es de carácter privado y contiene datos personales proporcionados por otra persona con un determinado interés³². En este caso, es de señalar que el actor autoriza a la autoridad y el demandado el uso de sus datos, al promover la querrela; y el demandado en todo momento tiene derecho –no solo en el emplazamiento- a que le comuniquen de los datos que de él obren en los ficheros de ésta autoridad.

Antes se hacía mención de que a principios del siglo XX, la cuestión de la protección de datos personales no era una preocupación importante para el individuo por el trabajo que implicaba el realizar una investigación exhaustiva de una persona. Sin embargo, hoy en día, no es un problema, ni tampoco un esfuerzo arduo el realizar una averiguación bastante pormenorizada de una persona, todo

³² El mismo derecho lo podemos ver en el art. 7.4 de la Convención Americana sobre derechos humanos (Pacto de San José), llevada a cabo en San José de Costa Rica, del 7 al 22 de noviembre de 1969.

gracias a la tecnología; por ejemplo, las notificaciones por edictos en periódicos oficiales son actualmente de fácil acceso a través de Internet.

El art. 14 refiere la esfera privada del individuo, al mencionar las excepciones de la publicidad de las audiencias en los Tribunales, es decir, los casos en que prima la privacidad a la publicidad. Este dispositivo señala que la prensa y el público podrán ser excluidos de la totalidad o parte de los juicios por consideraciones de moral, orden público o seguridad nacional en una sociedad democrática, así como cuando lo exija el interés de la vida privada de las partes (a juicio del Tribunal), o cuando por circunstancias especiales del asunto la publicidad pudiera perjudicar los intereses de la justicia. Asimismo, refiere que en materia penal o contenciosa todas las sentencias serán públicas, excepto aquellas en las que existan intereses de menores de edad que se contrapongan a dicha publicidad, así como las acusaciones en pleitos matrimoniales o de tutela de menores.

4.3 Declaración Americana de los Derechos y Deberes del Hombre

a) Antecedentes

La Declaración Americana de los Derechos y Deberes del Hombre (DADDH) -opacada meses después por la DUDH- de 2 de mayo de 1948 fue aprobada en el marco de la celebración de la novena conferencia internacional americana; aunque regional al igual que el Convenio Europeo de Derechos Humanos, la DADDH es el primer instrumento internacional de su tipo, ya que fue adoptada con antelación a la aprobación de la DUDH en el seno de las Naciones Unidas en diciembre del mismo año.

Tanto la Corte como la Comisión Interamericana de Derechos Humanos, han dictaminado que a pesar de haber sido adoptada como una declaración y no como un tratado, en la actualidad la Declaración Americana constituye una fuente de obligaciones internacionales para los Estados miembros de la Organización de Estados Americanos (OEA)³³.

³³ http://www.cidh.org/Basicos/Introduccion.htm#_ftn5 (consulta: 09/11/2012).

La Declaración, además de un preámbulo, comprende 38 artículos que definen los derechos protegidos y los deberes correlativos, e incluye un catálogo tanto de derechos civiles y políticos, así como de derechos económicos, sociales y culturales.

b) Objeto y fin

La Declaración es creada por la tradición de los pueblos americanos en dignificar a la persona humana, reconociendo en sus Constituciones que las instituciones jurídicas y políticas, rectoras de la vida en sociedad, tienen como objetivo principal la protección de los derechos esenciales del hombre, creando los medios que le permitan progresar espiritual y materialmente para alcanzar la felicidad.

En su preámbulo se advierte que la esencia de la Declaración es proteger los derechos con los que nace la persona, refiriendo que todos los hombres nacen libres e iguales en dignidad y derechos y, dotados como están por naturaleza de razón y conciencia, debiendo conducirse fraternalmente los unos con los otros (en toda actividad social y política del hombre). Aclarando que si los derechos exaltan la libertad individual, los deberes expresan la dignidad de esa libertad.

No obstante de ser ésta un instrumento de protección de derechos humanos de sistema regional, los Estados americanos han reconocido que los derechos esenciales del hombre no nacen del hecho de ser ciudadano de determinado Estado, sino que tienen como fundamento los atributos de la persona humana, que tienen su origen en la naturaleza misma. Así que los Estados americanos reconocen que, cuando el Estado legisla en esta materia, no crea o concede derechos sino que reconoce derechos que existían antes de la formación del Estado.

Asimismo, la DADDH en sus considerandos refiere que la protección internacional de los derechos humanos, debe de ser guiada por el derecho americano en evolución. Con esto último, los Estados americanos reconocen que no han alcanzado los mecanismos ideales de protección de los derechos fundamentales, y se refleja la intención para lograrlo, reconociendo que dicha

declaración atiende a las circunstancias sociales y jurídicas del momento, debiendo reforzarla, según las circunstancias, cada vez más en el campo internacional.

c) Contenido

El capítulo segundo de la Declaración es fundamental porque comprende los deberes del hombre, y es importante, porque si bien los derechos son fundamentales para el desarrollo de la persona ya que elevan su dignidad a través de los derechos humanos inherentes a la persona; también es importante que la persona esté consciente que el poseer derechos le implican, por correlación, una serie de deberes que debe de cumplir frente a quienes le rodean, tanto en su entorno social, como con el Estado³⁴.

La DADDH en su preámbulo especifica que los deberes de orden jurídico presuponen otros, de orden moral, que los apoyan conceptualmente y los fundamentan. Es deber del hombre servir al espíritu con todas sus potencias y recursos porque el espíritu es la finalidad suprema de la existencia humana y su máxima categoría. Es deber del hombre ejercer, mantener y estimular por todos los medios a su alcance la cultura, porque la cultura es la máxima expresión social e histórica del espíritu. Y puesto que la moral y buenas maneras constituyen la floración más noble de la cultura, es deber de todo hombre acatarlas siempre.

Así, el instrumento en análisis, se compone de dos capítulos que respectivamente contienen la regulación de los derechos y deberes de los americanos, aunque como lo aclara, el espíritu del instrumento es independiente de la nacionalidad respecto de un Estado, porque los derechos establecidos atienden al fundamento de los atributos de la persona humana. El contenido de los capítulos se conforma de la siguiente forma:

- *Capítulo Primero. Derechos.* Este apartado comprende el reconocimiento de distintos derechos tales como el derecho a la vida, a la libertad, a la

³⁴ Por ejemplo el pago de impuestos, los cuales deberán de ser siempre proporcionales al ingreso y actividad de la persona.

seguridad e integridad de la persona, de igualdad ante la ley, de libertad religiosa y de culto, libertad de investigación, opinión, expresión y difusión del pensamiento.

Asimismo, establece el derecho de protección a la honra, la reputación personal, así como de la *vida privada y familiar*, a la inviolabilidad del domicilio, así como el derecho a la inviolabilidad y circulación de la correspondencia. Protege también el derecho a la constitución y protección de la familia, a la maternidad y a la infancia, de residencia y tránsito. Además refiere el derecho a la preservación de la salud y al bienestar, a la educación, a los beneficios de la cultura, al trabajo y a una justa retribución, al descanso y a su aprovechamiento, a la seguridad social, al reconocimiento de la personalidad jurídica y de los derechos civiles.

Comprende los derechos de justicia, nacionalidad, sufragio y de participación en el gobierno, de reunión, de asociación, de propiedad, de petición, de protección contra la detención arbitraria. Garantiza el derecho a un proceso regular, de asilo y establece el alcance de los derechos del hombre, los cuales están limitados por los derechos de los demás, por la seguridad de todos y por las justas exigencias del bienestar general y del desenvolvimiento democrático.

- *Capítulo Segundo. Deberes.* Este apartado establece los deberes de las personas ante la sociedad, hacia los hijos y los padres, los de instrucción, de sufragio, de obediencia a la ley, de servir a la comunidad y a la nación, de asistencia y seguridad sociales, de pagar los impuestos, de trabajo y de abstenerse de actividades políticas en un país extranjero.

d) Artículo relacionado

La DADDH claramente garantiza el derecho a la privacidad mediante los artículos 5, 9 y 10³⁵, que establecen los derechos de protección de las personas

³⁵ El art. V establece que toda persona tiene derecho a la protección de la Ley contra los ataques abusivos a su honra, a su reputación y a su vida privada y familiar. Por su parte, el art. IX refiere que toda persona tiene el derecho a la inviolabilidad de su domicilio. Y por último el art. X dice que toda persona tiene derecho a la inviolabilidad y circulación de su correspondencia.

contra los ataques abusivos a su privacidad, entendida esta como su honra, reputación, vida privada y familiar, domicilio y correspondencia. La literalidad de los artículos referidos es la siguiente:

4.4 Convención Americana sobre Derechos Humanos

a) Antecedentes

El pacto de San José –como es también llamada la Convención- surge de la necesidad de regular la situación de los derechos humanos en el continente americano, independientemente de la nacionalidad. Es redactado durante la Convención Americana sobre Derechos Humanos celebrada en San José de Costa Rica, del 7 al 22 de noviembre de 1969, pero no es sino hasta 1978 que entra en vigor³⁶.

La Convención surge en el marco de los principios consagrados en la Carta de la Organización de los Estados Americanos, en la Declaración Americana de los Derechos y Deberes del Hombre, y en la Declaración Universal de los Derechos Humanos que han sido reafirmados y desarrollados en otros instrumentos internacionales, tanto de ámbito universal como regional.

b) Objeto y fin

La Corte refiere que el objeto y fin de la Convención no son el intercambio recíproco de derechos entre un número limitado de Estados, sino la protección de los derechos de todos los seres humanos en América, con independencia de la nacionalidad.

Asimismo, enfatiza que los tratados modernos sobre derechos humanos en general, y en particular la Convención Americana, no son tratados multilaterales de tipo tradicional concluidos en función de un intercambio recíproco de derechos para el beneficio mutuo de los Estados contratantes. Su objetivo es la protección de los derechos fundamentales, independientemente de su nacionalidad, resguardo que se podrá ejercer frente a su propio Estado, y frente a los otros Estados contratantes. Al aprobar estos tratados sobre derechos humanos,

³⁶ México ratificó la Convención el 24 de marzo de 1981, y se publicó en el DOF el 7 de mayo del mismo año.

los países se someten a un orden legal, que por el bien común asumen varias obligaciones, no en relación con otros Estados, sino en función de los individuos bajo su jurisdicción³⁷.

c) Contenido

La Convención se compone de tres partes, que comprenden varios capítulos con diferentes temas, y son los siguientes:

1. *Deberes de los Estados y derechos protegidos*: comprende la enumeración de deberes por parte de los Estados, los derechos civiles y políticos, los derechos económicos, sociales y culturales, así como la suspensión de garantías, interpretación y aplicación (de la Convención), y los deberes de las personas.
2. *Medios de protección*: describe a los órganos competentes, como la Comisión y la Corte Interamericana de Derechos Humanos, en su organización, funciones, competencia y procedimiento, e incluye un capítulo de disposiciones comunes para ambos órganos.
3. *Disposiciones generales y transitorias*: contiene los dispositivos relativos a la firma, ratificación, reserva, enmienda, protocolo y denuncia de la Convención; y las disposiciones transitorias concernientes a la Comisión y la Corte Interamericana de Derechos Humanos.

Es de interés el capítulo 2 de la primera parte del Pacto, referente a los derechos civiles y políticos, ya que regula el derecho a la privacidad en torno a la honra y la dignidad de la persona.

d) Artículo relacionado

La Convención Americana sobre Derechos Humanos³⁸, en el art. 11 con relación a la protección de la honra y de la dignidad, y siguiendo la misma línea de la DUDH, establece el derecho de todo individuo a que le sea respetado su

³⁷ Opinión consultiva de la Corte OC-2/82 de 24 de septiembre de 1982, relativa al efecto de las reservas sobre la entrada en vigencia de la Convención Americana sobre Derechos Humanos, solicitada por la Comisión Interamericana de Derechos Humanos.

³⁸ El Pacto de San José inicia su vigencia hasta el 18 de julio de 1978, casi nueve años después de que es redactada (<http://www.oas.org/juridico/spanish/tratados/b-32.html>, consulta: 09/11/2012).

honor y el reconocimiento de su dignidad. Agregando además, que nadie podrá 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, y que toda persona tiene derecho a la protección de la ley contra esas injerencias o esos ataques³⁹.

4.5 Convenio Europeo de Derechos Humanos

El Convenio de Roma de 4 de noviembre de 1950, para la protección de los derechos humanos y de las libertades fundamentales, al igual que otros instrumentos protectores de los derechos humanos, nace y se inspira a partir de la Declaración Universal de los Derechos Humanos. No obstante y habiéndola tenido de referente, el Convenio de Roma se presenta con un contenido material mucho menor (Ruiz Miguel, 2004: 93). Dicho documento en sus 18 artículos – referentes a los derechos y libertades- no contiene íntegramente los derechos consagrados en los 30 artículos de la DUDH. Si bien el Convenio ha sido criticado por ello, también es cierto que la Carta de los Derechos Fundamentales de la Unión Europea ha venido a subsanar e innovar la teoría de los derechos humanos⁴⁰.

a) Antecedentes

Los esfuerzos en favor de la unidad europea iniciaron el 5 de mayo de 1949 al constituirse el Consejo de Europa. La primera Asamblea Consultiva del Consejo de Europa inició sus reuniones en agosto del mismo año y también la elaboración de un Convenio para la protección de los derechos fundamentales. El 19 de agosto se comenzó el debate general en la Asamblea Europea del proyecto del Convenio. A lo largo de su tramitación se pusieron de manifiesto las discrepancias entre los “federalistas” europeos y los “estatalistas” nacionales. En los primeros días de noviembre de 1950 el Comité de Ministros se reunió en Roma y, ante la imposibilidad de llegar a un acuerdo unánime, no se recogieron todas las enmiendas hechas por la Asamblea Consultiva, desvirtuándose en gran

³⁹ Estos derechos, al igual que la Convención, son regulados por el art. 12 de la DUDH.

⁴⁰ Esta innovación en los derechos humanos se verá con posterioridad al abordar el tema de la Carta de los Derechos Fundamentales de la Unión Europea.

medida el texto a través de fórmulas de compromiso. Finalmente, el 4 de noviembre de 1950, se firmó en Roma el Convenio Europeo para la protección de los derechos humanos y las libertades públicas (CEDH), entrando en vigor el 3 de septiembre de 1953 (Ruiz Miguel, 2004: 18).

Con relación a los efectos posteriores de la aprobación del CEDH, el relativo fracaso del movimiento europeísta con la aprobación de un Convenio Europeo de Derechos Humanos que quedaba bastante lejos de lo que pedían los promotores de la unión política europea, fue un trauma para estos. A partir de ahí algunos promitentes europeístas decidieron emprender una vía alternativa, esto es lo que sugirió Robert Schuman apenas cinco días después de que se aprobara el CEDH⁴¹. En su declaración de 9 de noviembre de 1950 Schuman proclamó: “Europa no se hará de golpe, ni en una construcción de conjunto: se hará por medio de realizaciones concretas creando en primer lugar una solidaridad de hecho”. En esa misma declaración, Schuman, propuso dar el primer paso para conseguir una realización concreta, que creara esa solidaridad de hecho. De esta forma, recogiendo una idea que ya avanzó Coudenhove-Kalergi⁴² en 1923, propuso: “situar el conjunto de la producción franco-alemana de carbón y acero bajo una Alta Autoridad común, en una organización abierta a la participación de otros países de Europa”. Según Schuman esto será la “primera etapa de la Federación europea y cambiará el destino de las regiones volcadas durante largo tiempo en la fabricación de armas de guerra de las que son las más continuadas víctimas”. El llamamiento de Schuman dio origen a la Comunidad Europea del Carbón y del Acero (CECA), creada en París apenas un año después (1951) con la concurrencia de seis Estados (Alemania y Francia, Italia, Bélgica, Holanda y

⁴¹ Robert Schuman (29 de junio 1886 – 4 de septiembre 1963), político germano-francés, considerado como uno de los padres de Europa (en referencia a la Unión Europea), junto con Konrad Adenauer, Jean Monnet y Alcide de Gasperi. Se le conoce con el nombre de “Declaración Schuman” al discurso pronunciado por R. Schuman durante su encargo de Ministro de Asuntos Exteriores francés el 9 de Mayo de 1950, en el que se dio el primer paso para la formación de la Unión Europea, al proponer la administración conjunta de la CECA.

⁴² Richard Nikolaus Graf von Coudenhove-Kalergi (16 de noviembre 1894 – 27 de julio 1972), político y geopolítico austriaco, en 1923 publicó un manifiesto titulado *Pan-Europa* que supone la fundación de la Unión Internacional Paneuropeista, y con ella, el movimiento paneuropeo. La Unión Paneuropea Internacional dice ser el movimiento de unificación europeo más antiguo y es también conocido como el Movimiento Paneuropeo y el Movimiento Pan-Europa. Comienza con la publicación del manifiesto Paneuropa. Este movimiento trabaja con cuatro principios básicos: liberalismo, cristianismo, responsabilidad social y pro-europeísmo.

Luxemburgo). El tratado de la CECA era puramente económico y no incluía cláusulas políticas o relativas a los derechos fundamentales. La CECA inició un proceso de construcción europea económica distinto del proceso político patrocinado por el Consejo de Europa. Se bifurca así el intento de lograr la unidad europea. La bifurcación se hizo más llamativa por cuanto no coincidía el número de participantes en uno y otro proceso —el Consejo de Europa contaba con un número muy superior de Estados miembros— (Ruiz Miguel, 2004: 18-19).

b) Objeto y fin

Los países miembros del Consejo de Europa, entonces únicamente 13 al momento de la firma el 4 de noviembre de 1950⁴³, en el marco de la DUDH, consideraron necesario crear un instrumento que garantizara los derechos humanos de los ciudadanos de los países de la Unión Europea y de todos aquellos que se quisieran adherir.

El CEDH es de aplicación universal, porque tal y como se establece en el primer artículo, las partes contratantes reconocen a toda persona dependiente de su jurisdicción los derechos y libertades definidos en el título primero del Convenio. Así los Estados partes se comprometen entre sí a proteger los derechos de las personas, y no solo los de sus ciudadanos, sino los de todas aquellas que se encuentren bajo la jurisdicción de alguno de los Estados parte de la Convención.

Los fundadores del Consejo de Europa contaron con el marco de referencia, cuyo propósito era evitar el surgimiento de nuevas dictaduras y nuevos desastres ocasionados por guerras; integrado por los principios y objetivos comunes, así como por la voluntad de salvaguardarlos y difundirlos a través de una organización que los encarnara. Los principios eran la preeminencia del Derecho y el respeto de los derechos humanos, y entre los objetivos estaban el proteger y reforzar la democracia pluralista, así como, favorecer el desarrollo de una verdadera identidad europea (García Jiménez, 1998: 26-27).

⁴³ Alemania, Austria, Bélgica, Dinamarca, Francia, Holanda, Irlanda, Islandia, Italia, Luxemburgo, Noruega, Reino Unido y Turquía (García Jiménez, 1998: 249-250). El Convenio Europeo de Derechos Humanos entró en vigor el 3 de septiembre de 1953. El convenio fue ratificado por España el 26 de septiembre de 1979 y publicado en el Boletín Oficial del Estado el 10 de octubre de 1979.

La finalidad del Convenio la constituye la protección efectiva de los derechos humanos, y no así, la creación de obligaciones recíprocas entre las partes (García Roca y Santolaya, 2005: 29). Por lo tanto, la función del Tribunal Europeo de Derechos Humanos (TEDH) radica en la interpretación del Convenio y sus protocolos, fijando ciertas normas internacionales que los Estados deber respetar, respecto de las personas bajo su jurisdicción, tal y como se establece en el artículo primero de la Convención⁴⁴.

El Convenio –dice el TEDH- va más allá de un mero compromiso recíproco entre los Estados contratantes, ya que crea toda una red mutua de compromisos bilaterales y obligaciones objetivas, las cuales –como se establece en el preámbulo- son de aplicación colectiva. Por lo tanto, el Convenio permite a los Estados contratantes exigir el cumplimiento de dichas obligaciones sin tener que justificar un interés derivado⁴⁵. De la traducción de los textos resulta ambiguo distinguir entre el “mero compromiso recíproco” y los “compromisos bilaterales”, pero, en este caso considero que es importante prestar atención a la frase “obligaciones objetivas” (las cuales son de mayor jerarquía que los “meros compromisos recíprocos”), éstas son las que permiten el debido cumplimiento del CEDH.

Un aspecto importante del CEDH, es el hecho de ser considerado por el TEDH como un Instrumento vivo que debe de ser interpretado a la luz de las condiciones actuales, que podrá ser influenciado por los estándares comúnmente aceptados por los Estados miembros, y que dicho Convenio deberá aplicarse en concordancia con el desarrollo de los derechos humanos en el Derecho Internacional⁴⁶. Por lo tanto, tenemos un instrumento protector, que no es diferente de los demás, sin embargo, se caracteriza porque el máximo Tribunal garante de dicho instrumento (TEDH), se ha pronunciado en favor de una

⁴⁴ STEDH de 9 de febrero de 1967, en el caso del régimen lingüístico de la enseñanza en Bélgica.

⁴⁵ STEDH Irlanda contra Reino Unido, de 18 de enero de 1978.

⁴⁶ Este criterio del TEDH puede verse en diferentes sentencias, las que particularmente han sido consultadas son las pronunciadas en el caso Henaf contra Francia de 27 de noviembre de 2003, relativa al encadenamiento en cama de un delincuente reincidente, sin antecedentes de violencia para que tal medida fuese tomada (§55); la Sentencia del caso Tyrer contra Reino Unido de 25 de abril de 1978 (§31); y la del caso Saadi contra Reino Unido de 29 de Enero de 2008 (§55).

interpretación de tipo *ad hoc* con el tiempo y la sociedad que regula, al considerarlo como un documento vivo, que avanza y evoluciona.

c) Contenido

El Convenio se encuentra compuesto por tres títulos: 1) derechos y libertades, 2) Tribunal Europeo de Derechos Humanos, y 3) disposiciones diversas. Los temas que refiere el Convenio en cada uno de sus títulos son los siguientes:

- *Título I Derechos y Libertades:* en esta parte, el ordenamiento regula la protección de los derechos humanos como: el derecho a la vida, la prohibición de la tortura, de la esclavitud y del trabajo forzado, el derecho a la libertad y la seguridad, el derecho a un proceso equitativo. Regula además el principio de no haber pena sin ley, así como el derecho al respeto de la *vida privada y familiar*, la libertad de pensamiento, de conciencia y de religión, la libertad de expresión, libertad de reunión y de asociación, el derecho a contraer matrimonio, el derecho a un recurso efectivo, la prohibición de discriminación, la derogación en caso de estado de excepción, las restricciones a la actividad política de los extranjeros, la prohibición del abuso del derecho, y la limitación en el uso de las restricciones de derechos.
- *Título II Tribunal Europeo de Derechos Humanos:* en este amplio apartado el Convenio regula todo lo relativo a los órganos operativos, es decir, a la Institución del Tribunal, el número de jueces, las condiciones de ejercicio de sus funciones, la elección de los jueces, la duración del mandato, así como la revocación del mismo. Regula además, la Secretaría y referendarios, el Pleno del Tribunal, los Comités, Salas y Gran Sala, la declaración de inadmisibilidad por los comités, las resoluciones de las salas sobre la admisibilidad y el fondo del asunto. También refiere la inhibición a favor de la Gran Sala, las atribuciones de la Gran Sala, la competencia del Tribunal, los asuntos presentados por los Estados, las demandas individuales, las condiciones de admisibilidad, la intervención de terceros, los archivos de las demandas, el examen contradictorio del asunto y el

procedimiento de arreglo amistoso. Codifica además la conclusión de un arreglo amistoso, la vista pública y acceso a los documentos, la satisfacción equitativa, las sentencias de las Salas, la remisión ante la Gran Sala, las Sentencias definitivas, la motivación de éstas y las resoluciones, así como la fuerza obligatoria y la ejecución de las mismas, las opiniones consultivas, la competencia consultiva del Tribunal, la motivación de las opiniones consultivas, los gastos del funcionamiento del Tribunal, y los privilegios e inmunidades de los Jueces.

- *Título III Disposiciones diversas:* en este último capítulo se encuentra la regulación de las encuestas del Secretario General, la protección de los derechos humanos reconocidos, los poderes del Comité de Ministros, la renuncia a otros modos de solución de controversias, la aplicación territorial, las reservas, la denuncia, así como la firma y ratificación del Convenio.

Los derechos y libertades reconocidos en el título primero del Convenio ponen de manifiesto dos datos importantes: en primer lugar, que tales derechos y libertades se enuncian mediante conceptos jurídicos indeterminados, llamados a ganar concreción en la aplicación del Convenio a casos concretos; y en segundo lugar, que el Convenio protege fundamentalmente derechos civiles y políticos – derechos de primera generación–, aunque alguno de ellos –como la libertad de sindicación– tengan la indiscutible dimensión social y económica. Esto último, se debió a que se procedió por etapas, protegiendo primero los derechos fundamentales sin los cuales los sistemas pluralistas de Estados democráticos de Derecho no pueden funcionar. Y que en el Consejo de Europa los derechos sociales son objeto de reconocimiento y protección en la Carta Social de Europa, adoptada en Turín el 18 de octubre de 1961 y entrada en vigor en 1965 (Carrillo Salcedo, 2003: 23-24).

d) Artículo relacionado

El art. 8 del Convenio Europeo de Derechos Humanos establece la garantía del derecho a la vida privada y familiar, asimismo, el respeto al domicilio y a la correspondencia. Como producto de la tecnología, con

posterioridad, la Carta de los Derechos Fundamentales de la Unión Europea sustituye el concepto de “correspondencia” por el de “comunicaciones” (tema que se abordará en páginas siguientes).

Asimismo, el art. 8.2 CEDH continua señalando que no podrá haber injerencia de la autoridad pública en el ejercicio del derecho a la vida privada, salvo cuando 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 de las infracciones penales, la protección de la salud o de la moral, o la protección de los derechos y las libertades de terceros.

El CEDH sigue la línea directriz de la DUDH, sin embargo varía en el ámbito de protección de derechos y no incluye en su redacción el respeto a la honra o reputación, en lo concerniente a la tutela del derecho a la vida privada. No obstante el honor y la reputación no están directamente protegidos por el Convenio, el art. 10.2 incluye la protección de la reputación como causa legítima contra la injerencia en la libertad de expresión; y añade además que la doctrina, de los órganos de supervisión del Convenio, admite que un ataque a la reputación de una persona puede constituir una violación del art. 8.1 (Lasagabaster Herrarte, 2004: 255). Otros instrumentos (como la DUDH, la DADDH y la CADH) refieren la honra y la reputación como bien jurídicamente protegido por el derecho a la privacidad, el CEDH no los incluye en el ámbito de su tutela, es por ello se podría pensar que el alcance de dicho dispositivo se ve limitado en comparación con otros instrumentos.

Este art. 8 CEDH como protector del derecho a la privacidad, ha sido ampliamente desarrollado por el Tribunal, de forma por demás interesante, en lo que respecta a la vida privada y familiar con las Sentencias de los casos de transexualidad y homosexualidad⁴⁷, en relación con el art. 14 que prohíbe todo

⁴⁷ Por no ser el tema central de la investigación no se entra al estudio de la privacidad en estos aspectos, sin embargo y para mayor ilustración se pueden consultar sobre eliminación de las discriminaciones en el tratamiento penal y sancionador de la homosexualidad, las Sentencias de los casos: Dudgeon contra el Reino Unido de 22 de octubre de 1981, Norris contra Irlanda de 26 de octubre de 1988, Modinos contra Chipre de 22 de abril de 1993, A.D.T. contra el Reino Unido de 31 de Julio de 2000. Así también, Sobre la edad para el consentimiento necesario para

tipo de discriminación y con el art. 12 que consagra el derecho a casarse y formar una familia.

Hasta este punto, se ha visto como los ordenamientos internacionales que garantizan el derecho a la privacidad, asumen únicamente la protección de esta en lo concerniente a la vida privada, a la familiar, y en lo que respecta al domicilio y la correspondencia.

En lo que hace a la protección del derecho a la vida privada, contemplada por el art. 8 CEDH, también comprende la protección de los datos personales. Este último derecho, deriva del derecho a la privacidad, pero se estudia en pocas sentencias del TEDH, por ejemplo: Peck Vs. Reino Unido, L.L. Vs. Francia, I. Vs. Finlandia, S. y Marper Vs. Reino Unido, Segerstedt-Wiberg y otros Vs. Suecia, Amann Vs. Suiza y Perry Vs. Reino Unido; en éstas se declara que ha habido una violación al art. 8 CEDH⁴⁸

4.6 Convenio No. 108 para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal.

El Convenio No. 108 del Consejo de Europa para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, nació el 28 de enero de 1981 con el propósito de garantizar a los ciudadanos de los Estados contratantes, el respeto de sus derechos y libertades, en concreto, el derecho a la vida privada, frente a los tratamientos de datos personales, conciliando el respeto a la vida privada y a la libre circulación de información

mantener relaciones heterosexuales o lésbicas, las sentencias de los casos: L y V contra Austria y S.L contra Austria, ambas del 9 de enero de 2003. Sobre casos de expulsión de las fuerzas armadas por motivo de homosexualidad, los casos Smith y Grady contra el Reino Unido, de 27 de septiembre de 1999, Lusting-Perean y Beckett contra el Reino Unido de 27 de septiembre de 1999, Perkins y R. contra el Reino Unido de 22 de octubre de 2002, Beck, Copp, y Bazeley contra el Reino Unido de 22 de octubre de 2002. Así como la obligación positiva de modificar el acta de nacimiento de una persona por haber cambiado de sexo, problema planteado varias ocasiones y rechazado por el Tribunal durante las décadas de los 80's y 90's; ésta línea se supera jurisprudencialmente en los casos I contra Reino Unido y Christine Goodwin contra el Reino Unido, ambas del 11 de julio del 2002. El caso Van Kück contra Alemania de 12 de junio de 2003, contraria al Convenio la negativa de las autoridades alemanas a rembolsar los gastos médicos derivados del cambio de sexo del recurrente.

⁴⁸ Para estudio se refieren dos sentencias, la más antigua y la más reciente, ambas aparecen en el archivo electrónico que puede ser consultado en la página web del TEDH.

entre los Estados⁴⁹. Para ello, a diferencia de lo que ocurrió con las Resoluciones del Comité de Ministros, se le dotó, en tanto que Convenio internacional, de carácter vinculante y, por lo tanto, de fuerza normativa obligatoria. En este sentido, aunque se haya argumentado que el Convenio 108 no supuso una innovación frente a los textos anteriores, su gran aportación fue otorgar fuerza vinculante a los principios generales de la protección de datos establecidos en las Resoluciones (73) 22 y 74 (29) (Arenas Ramiro, 2006: 155)⁵⁰.

a) Antecedentes

En este documento los estados miembros del Consejo de Europa consideran 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 en cuenta la intensificación de la circulación a través de las fronteras de los datos de carácter personal que son objeto de tratamientos automatizados.

b) Objeto y fin

El artículo primero del Convenio establece que el fin es garantizar, en el territorio de cada Parte, a cualquier persona física sean cuales fueren su nacionalidad o residencia, el respeto de sus derechos y libertades fundamentales concretamente su derecho a la vida privada, con respecto al tratamiento automatizado de los datos de carácter personal correspondientes a dicha persona (“protección de datos”).

c) Contenido

⁴⁹ Antes del Convenio 108 existían legislaciones en materia de protección de datos, entre las que se encuentran la ley sueca de 11 de mayo de 1973, la alemana del 27 de enero de 1977, la ley francesa del 6 de enero de 1978, las leyes danesas del 8 de junio de 1978, la ley noruega del 9 de junio de 1978, la ley austriaca del 18 de octubre de 1978, y la ley de Luxemburgo del 31 de marzo de 1979 (Suñé Llinás, 2002: 57-69 y Domínguez González, 2010: 169).

⁵⁰ Para mayor abundamiento sobre las Resoluciones del Consejo de Europa (73) 22 y 74 (29) véase Arenas Ramiro (2006: 151-152). Por otro lado, la maestra Arenas Ramiro (2006: 156) dice que la firma del Convenio 108 no proporcionó la suficiente protección homogénea en materia de protección de datos que se había esperado. Esto se debió esencialmente a la naturaleza del Convenio: el mismo, a pesar de tener una naturaleza vinculante, establecía únicamente unos principios mínimos, permitiendo que, posteriormente, fueran los Estados firmantes los que los desarrollaran.

El Convenio 108 consta de un Preámbulo y de 27 artículos distribuidos en 7 Capítulos. En el Capítulo I se recoge el objeto del Convenio; en el Capítulo II, los principios que deben regir la calidad de los datos (lealtad, finalidad, pertinencia, exactitud y conservación) y los derechos de los titulares de los datos (información, acceso, rectificación y cancelación, y el derecho a recurrir); en el Capítulo III se regulan los flujos transfronterizos de datos; en el Capítulo IV, los mecanismos de cooperación entre las Partes; en el Capítulo V se desarrolla la estructura y funcionamiento del “Comité Consultivo”⁵¹; en el Capítulo VI se regulan los procedimientos para la presentación y aprobación de Enmiendas; y el Capítulo VII recoge las Cláusulas finales, relativas a la entrada en vigor del Convenio y a la adhesión al mismo de Estados no miembros del Consejo de Europa.

4.7 Directiva de 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.

En el ámbito comunitario, se cuenta con 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, acordada por los Estados miembros para asegurar el debido control y seguridad del flujo de datos de las personas (Borchardt, 2000: 66)⁵².

a) Antecedentes

Este instrumento es la norma marco sobre protección de datos en la esfera comunitaria. A diferencia del Convenio no. 108, al que completa, no es directamente un instrumento de protección de las personas, sino que se concibe

⁵¹ Órgano asesor encargado de impulsar y supervisar la actuación del Convenio 108.

⁵² La directiva y el reglamento, son los instrumentos más importantes de la actuación comunitaria. Intentan combinar la necesaria unidad del Derecho Comunitario con el mantenimiento de la variedad de las peculiaridades nacionales. La directiva sólo es obligatoria para los Estados miembros respecto del objetivo que propone, dejando a su elección la forma y los medios para alcanzar los objetivos establecidos a escala comunitaria en el marco del ordenamiento jurídico nacional. Aun cuando estos tienen libertad para elegir la forma y los medios de transposición, se evaluará si las disposiciones correspondientes han sido incorporadas conforme al Derecho Comunitario con arreglo a los criterios del propio ordenamiento comunitario.

como una herramienta para impedir las trabas a la libre circulación de información en el mercado interior (Guerrero, 2006: 63-64).

Es interesante el considerando -dentro de los múltiples de este instrumento- que refiere que cuando un país tercero no ofrezca un nivel de protección adecuado debe prohibirse la transferencia al mismo de datos personales. Y es particular, porque al no existir una normativa que regule la materia en un país determinado, produce la obstrucción de las transacciones. Sin embargo, la Directiva va más allá previendo la forma de paliar este obstáculo y lo desarrolla en el Capítulo IV de la misma.

b) Objeto y fin

El objeto de la Directiva es que los Estados miembros garanticen, con arreglo a las disposiciones de la misma, 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 datos personales. Así como, el que los Estados no puedan restringir ni prohibir la libre circulación de estos datos entre los demás Estados miembros por motivos relacionados con la protección garantizada en virtud del apartado 1.

c) Contenido

La Directiva consta de una sección amplia de considerando y de 34 artículos distribuidos en 7 Capítulos. En el Capítulo I se recogen las disposiciones generales de la Directiva (objeto, definiciones, ámbito de aplicación y derecho nacional aplicable); en el Capítulo II, las condiciones generales para la licitud del tratamiento de datos personales (principios relativos a la calidad de los datos, a la legitimación del tratamiento de datos, las categorías especiales de tratamientos, la información del interesado, el derecho de acceso del interesado a los datos, las excepciones y limitaciones, el derecho de oposición del interesado, la confidencialidad y seguridad del tratamiento y la notificación); en el Capítulo III regula los recursos judiciales, responsabilidad y sanciones; en el Capítulo IV, la

transferencia de datos personales a países terceros⁵³; en el Capítulo V se desarrollan los códigos de conducta; el Capítulo VI es sobre la autoridad de control y grupo de protección de las personas en lo que respecta al tratamiento de datos personales; el Capítulo VII recoge las medidas de ejecución comunitarias; y por último, las disposiciones finales, relativas a la observancia de la Directiva por parte de los Estados miembros.

4.8 Carta de los Derechos Fundamentales de la Unión Europea

La Carta surge en el año 2000 como un instrumento único por su innovación, en el que se reconocen derechos producto de la nueva realidad y formas de vivir de la sociedad actual, como el derecho a la protección de datos personales; asimismo, este documento limita actividades científicas, a modo de prevención inmediata de los experimentos en personas, tales como la clonación; aparecen también derechos medio ambientales, etc.

a) Antecedentes

En el Consejo Europeo de Colonia celebrado el 3 y 4 de junio de 1999, se adoptó una decisión sin precedentes, la elaboración de una Carta de Derechos Fundamentales de la Unión. En concreto se consideró que: “La salvaguardia de los derechos fundamentales es uno de los principios básicos de la Unión Europea y una condición indispensable para la legitimidad de la misma. El Tribunal de Justicia Europeo ha confirmado y configurado, con su jurisprudencia, la obligación de la Unión de velar por los derechos fundamentales. La evolución actual de la Unión exige la redacción de una Carta de derechos fundamentales que permita poner de manifiesto ante los ciudadanos de la Unión la importancia sobresaliente de los derechos fundamentales y su alcance”⁵⁴.

La configuración de los derechos fundamentales hecha por el Tribunal de Justicia, es desarrollada desde los años setenta en una –ahora ya abundante–

⁵³ Para profundizar en el tema de transferencia internacional de datos personales véase a Sancho Villa (2003).

⁵⁴ Decisión del Consejo Europeo, relativa a la elaboración de una Carta de Derechos Fundamentales de la Unión Europea, anexo 4 de las conclusiones de la Presidencia del Consejo Europeo de Colonia, celebrado los días 3 y 4 de junio de 1999. Boletín de la Unión Europea No. 6/1999.

jurisprudencia que incorpora, en el Derecho Comunitario, la protección de estos derechos por la vía de los principios generales del Derecho, como único vehículo jurídico posible en ausencia de disposiciones expresas en los Tratados (Pi Lorens, 2001: 14).

Es decisión del Consejo Europeo también que: “esta Carta deberá incluir los derechos de libertad e igualdad y los principios procesales fundamentales, tal como se recogen en el Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales y como resultan de las tradiciones constitucionales comunes de los Estados miembros, como principios generales del Derecho comunitario. La Carta deberá contener asimismo los derechos básicos que corresponden únicamente a los ciudadanos de la Unión. Al redactar la Carta, se tendrán en cuenta también los derechos económicos y sociales, del mismo modo que en la Carta Social Europea y en la Carta comunitaria de los derechos sociales fundamentales de los trabajadores (art. 136 TCE), en cuanto no se limitan a fundamentar los objetivos de la actuación de la Unión”. De este modo, en dicho Consejo Europeo se sentaron las bases de lo que debían de ser los rasgos esenciales de este documento.

Así que, en Colonia se otorgó a un órgano llamado Convención (presidido por Alemania) el mandato de redactar el proyecto de la Carta. Este se constituyó en diciembre de 1999 y aprobó el proyecto el 2 de octubre del 2000, mismo que días después, habría de ser aprobado por el Consejo de Europa de Biarritz el 13 y 14 de octubre, mediante acuerdo unánime, transmitiéndolo al Parlamento Europeo y a la Comisión. El Parlamento Europeo dio su acuerdo el 14 de noviembre de 2000 y la Comisión, el 6 de diciembre de 2000. Finalmente, los Presidentes del Parlamento Europeo, del Consejo y de la Comisión, en nombre de sus Instituciones, firmaron y proclamaron la Carta el 7 de diciembre de 2000 en Niza.

b) Objeto y fin

Es importante que cada Estado cuente con un cuerpo normativo que esté de acuerdo con la realidad de la sociedad que regula, por ello, el Preámbulo de la Carta establece claramente la necesidad de reforzar la protección de los derechos

fundamentales conforme a la evolución de la sociedad, del progreso social y, de los avances científicos y tecnológicos.

La Carta es una contribución al compromiso de la UE por la preservación y el fomento de los valores comunes dentro de la diversidad de culturas y tradiciones de los pueblos de Europa. Su texto establece que la Unión está fundada sobre los valores indivisibles y universales de la dignidad humana, libertad, igualdad y la solidaridad, y se basa en los principios de la democracia y del Estado de Derecho⁵⁵.

c) Contenido

La CDF se integra por 54 artículos en siete capítulos, dentro de los cuales se desglosan distintas disposiciones que protegen la dignidad, libertad, igualdad, solidaridad, justicia y ciudadanía. El contenido de cada uno de los siete apartados es el siguiente:

- *Capítulo I. DIGNIDAD.* Se establece la protección y respeto a la dignidad humana, así mismo se fija el derecho a la vida, a la integridad de la persona, la prohibición de la tortura y de las penas o los tratos inhumanos o degradantes, así como la prohibición de la esclavitud y del trabajo forzado.
- *Capítulo II. LIBERTADES.* Se funda el derecho a la libertad y a la seguridad, el respeto a la vida privada y familiar, el *derecho a la protección de datos de carácter personal*, el derecho a contraer matrimonio y derecho a fundar una familia, se establece además la libertad de pensamiento, de conciencia y de religión. Se asientan las libertades de expresión y de información, de reunión y de asociación, de las artes y de las ciencias, de empresa, la libertad profesional y derecho a trabajar, el derecho a la educación, a la propiedad, de asilo, así como la protección en caso de devolución, expulsión y extradición.

⁵⁵ Se asume con normalidad que el depósito de derechos fundamentales vigente en un Estado puede incrementarse, sin tocar el texto de la Constitución a través de instrumentos internacionales. Por ello, y a decir por Martín-Retortillo Baquer (2009: 142), el sistema constitucional español de derechos humano, es un sistema abierto, y para mejorar puede irse complementando gradualmente a través de instrumentos internacionales. Así que –continúa diciendo–, cuando se culmine el proceso y entre en vigor la Carta de Derechos Fundamentales, lo que de una parte va a representar el incremento del acervo de derechos fundamentales vigentes en España, de otra parte también implica que el Estado asume compromisos y cargas que antes no tenía (de ahí que algunos Estados, precisamente para evitar compromisos derivados del nuevo texto, hayan formulado sus reservas a la hora de formalizar la ratificación, por ejemplo Polonia y Reino Unido).

- *Capítulo III. IGUALDAD.* Se contempla la igualdad ante la ley, la no discriminación, el respeto a la diversidad cultural, religiosa y lingüística. Se establece además la igualdad entre hombres y mujeres, los derechos del menor, los derechos de las personas mayores y la integración de las personas discapacitadas.
- *Capítulo IV. SOLIDARIDAD.* Se establece el derecho a la información y consulta de los trabajadores en la empresa, de negociación y de acción colectiva, de acceso a los servicios de colocación, de protección en caso de despido injustificado, las condiciones de trabajo justas y equitativas, la prohibición del trabajo infantil y la protección de los jóvenes en el trabajo, la protección de la vida familiar y profesional, la seguridad social y ayuda social, la protección de la salud, el acceso a los servicios de interés económico general, la protección del medio ambiente y la de los consumidores.
- *Capítulo V. CIUDADANIA.* Se instituye el derecho a ser elector y elegible en las elecciones al Parlamento Europeo, el derecho a ser elector y elegible en las elecciones municipales, el derecho a una buena administración, derecho de acceso a los documentos, el derecho a someter al Defensor del Pueblo de la Unión los casos de mala administración, el derecho de petición, la libertad de circulación y de residencia, así como la protección diplomática y consular.
- *Capítulo VI. JUSTICIA.* Se establece el derecho a la tutela judicial efectiva y a un juez imparcial, se fija la presunción de inocencia y derechos de la defensa, los principios de legalidad y de proporcionalidad de los delitos y las penas, así como el derecho a no ser acusado o condenado penalmente dos veces por el mismo delito.
- *Capítulo VII. DISPOSICIONES GENERALES.* Aquí se regula el ámbito de aplicación, el alcance de los derechos garantizados, el nivel de protección y la prohibición del abuso de derecho.

La Carta de los Derechos Fundamentales de la Unión Europea (proclamado en Niza el 7 de diciembre de 2000), en su capítulo II relativo a las

libertades, consagra como se han señalado diferentes derechos y libertades, entre las que se encuentra como novedad el tema principal de nuestro estudio: “el derecho a la protección de datos personales”. En la Carta se establece, por primera vez, como derecho fundamental del individuo, aquello que antes se había visto discretamente y como mera interpretación del derecho a la privacidad, pero es hasta este momento, en el que se consolida como uno de los derechos fundamentales de la persona.

El preámbulo de la CDF establece que es necesario dotar a los Estados miembros de mayor presencia y de reforzar la protección de los derechos fundamentales al tenor de la evolución de la sociedad, del progreso social y de los avances científicos y tecnológicos. Por ello, la Carta esboza de modo muy concreto y eficaz los derechos fundamentales, inspirada principalmente de las tradiciones constitucionales comunes de los Estados miembros.

Al igual que los diferentes ordenamientos que se han desarrollado con anterioridad, en el art. 6 CDF se reconocen los derechos de libertad y de seguridad, y en el art. 7 CDF el derecho al respeto de la vida privada y familiar, agregando en el mismo dispositivo, el respeto del domicilio y, como novedad, se establece el respeto de la persona en sus “comunicaciones”⁵⁶. Es aquí –como se señaló con anterioridad–, que la redacción del texto no pierde de vista la realidad tecnológica y atiende a los avances de las telecomunicaciones, adecuándose a la contemporaneidad de su redacción, y sustituye el término de “correspondencia” por el de “comunicaciones”, que es más apropiado a la realidad tecnológica.

Es de recordar que el servicio de correo ordinario, hace varias décadas dejó de ser el principal medio de comunicación por el que se transfería una gran cantidad de información. En la actualidad, existe una amplia gama de instrumentos que han sido rápidamente aceptados por la sociedad debido a la facilidad para acceder a ellos. Entre los medios de comunicación y transferencia de datos más populares destacan: el fax, la telefonía fija y móvil, el correo electrónico, la señal “*bluetooth*” e internet, además de aquellos dispositivos

⁵⁶ Art. 7 CDF. 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.

destinados al almacenamiento electrónico de información (*tablets, smartphones, usb*, servidores en la nube, etc.). Todos ellos, constituyen hoy en día, los canales más importantes de transferencia de datos personales, siendo los medios electrónicos los que se encuentran en la punta de la transferencia de bases completas de datos, dada su practicidad satelital, inalámbrica y de fácil transportación.

En ocasiones, debido al desconocimiento de las nuevas tecnologías y al experimentar con ellas, se proporciona una gran cantidad de información personal a diferentes receptores, quienes al captarla disponen de ella de un modo desconocido para los emisores, quedando estos últimos, en un estado de indefensión ante el uso que el receptor haga de sus datos. El art. 7 CDF se encuentra un paso adelante de los demás textos protectores de los derechos fundamentales –en relación con la protección de datos personales–, al reconocer la importancia del derecho a proteger la vida privada y familiar, mediante el respeto a las comunicaciones, que se realizan a través de la utilización de diversos medios.

d) Artículo relacionado

El art. 8 CDF reconoce y eleva explícitamente a la categoría de derecho fundamental la protección de datos personales. Asimismo, hace referencia a que el tratamiento de la información sea leal, para los fines concretos de recopilación y sobre la base del consentimiento de la persona afectada; igualmente menciona que toda persona tiene el derecho de acceso y rectificación de los datos recogidos que le conciernan. En la última fracción de este artículo se prevé que el respeto de estas normas quedará sujeto al control de una autoridad independiente. Así, este documento constituye un parte-aguas en materia de protección de datos personales⁵⁷.

⁵⁷ Art. 8 CDF. 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 su rectificación. 3. El respeto de estas normas quedará sujeto al control de una autoridad independiente.

II. EL DERECHO A LA PROTECCION DE DATOS PERSONALES Y SUS PRIMERAS INSERCIONES CONSTITUCIONALES

1. Generalidades de la Protección de Datos Personales.

A partir del desarrollo de las nuevas tecnologías, los datos personales contenidos en ficheros –principalmente electrónicos- se vuelven cada vez más vulnerables a la apropiación y abuso, de aquellos que poseen o acceden a las bases de datos. Las oportunidades de tratamiento de la información que ofrece la informática amplían la posibilidad de que el ciudadano pierda su anonimato. Por este motivo se protege la puesta en común de datos aparentemente inocuos, frente a ilimitados almacenamientos, tratamiento y transferencias que se refieran a un individuo o que puedan ser individualizados (González Pascual, 2009: 948).

Por ello, el Estado, propietario de grandes bases de datos, y la Comunidad Internacional, ante el flujo de datos que día a día se transfieren en ámbitos principalmente comerciales, deben de ser los impulsores de la normatividad correspondiente en la materia⁵⁸.

La protección de datos personales, es un derecho fundamental relativamente nuevo, y configurado a partir de las concepciones que se tienen de la vida privada o intimidad, del derecho al honor y del derecho a la propia imagen⁵⁹. La evolución de estos derechos, principalmente el de la vida privada, han planteado nuevas situaciones que habrán de ser motivo de la creación de un nuevo derecho, la protección de datos personales.

⁵⁸ Hoy en día, el principal promotor de la normatividad relativa a la protección de datos personales es la Unión Europea, la cual ha impulsado a países de todo el mundo, como Argentina en Latinoamérica, convirtiéndose actualmente en el país que más ha desarrollado el tema, en su doble aspecto doctrinal y jurídico.

⁵⁹ El derecho al honor y a la propia imagen, como la protección de datos personales, son derechos independientes entre sí, sin embargo, y como ocurre con otros derechos, se relacionan entre sí, principalmente con el derecho a la vida privada. Desde una perspectiva se podría decir que el derecho a la privacidad es el género, mientras que los otros son la especie –cada uno en su propio ámbito de aplicación–. Lo anterior, ya que la vulneración de alguno afecta directamente la vida privada de la persona. Pero hay que recordar, que en el caso particular del derecho a la protección de datos personales, comprende el control por parte de la persona de su información personal, que puede o no, ser privada.

El estudio de este derecho se sitúa en el campo de los derechos fundamentales, y por ello es importante comprender su nueva inclusión dentro del catálogo de los mismos, como un derecho nuevo, ya sea como derecho a la protección de datos personales o como autodeterminación informativa (Conde Ortiz, 2005: 27).

Algo sabido, es que hoy en día las vulneraciones de la intimidad, cada vez se presentan de forma más grave por la obtención de perfiles personales. El Tribunal Constitucional alemán en su Sentencia de 1983 contra la Ley del censo, establecía que en virtud de la evolución de los condicionamientos tecnológicos, a través de los perfiles personales, era posible producir una imagen total y pormenorizada de una persona, incluso en el ámbito de su intimidad; convirtiendo a su propio ciudadano, en el llamado (así citado por el propio Tribunal) «hombre de cristal»⁶⁰. Este término, significaba la pérdida del anonimato, porque el individuo se convertía en una persona conocida y por lo tanto frágil en el aspecto más profundo de su vida, es decir, su intimidad. Por ello, no resulta extraño, la notoria necesidad de la protección de los perfiles personales, entendidos estos hoy en día, como los datos personales contenidos en los ficheros o registros almacenadores de grandes bases de datos, información mediante la cual se podría hacer un retrato de la persona. Fioriglio (2008: 78-86) refiere que la “*profilazione*”, es uno de los grandes problemas de Internet, y lo define en general como la clasificación del comportamiento, el rastro de gustos, ideología, intereses, etc. que se deja en la red, y recuerda aquello de que cada uno es seguido por su pasado. Y las *cookies* que se almacenan en los portátiles contribuyen a la *profilazione*.

Para el estudio de la protección de datos personales, Campuzano Tome (2000: 55) refiere que el tema de la salvaguardia de la vida privada y de los datos personales puede ser analizado desde una doble vertiente: la primera, que corresponde a la protección de los datos personales como *objeto de valor* en un sistema de mercado dirigido a instaurar el comercio electrónico en cuanto principal sistema de intercambio de bienes. En tal caso, se habla de *protección a*

⁶⁰ Sentencia del Tribunal Constitucional alemán, de fecha 15 de diciembre de 1983, en contra de la Ley del Censo. Boletín de Jurisprudencia Constitucional No. 33, 1984. p. 137-138.

los consumidores, de protección de los datos relativos al consumo, de protección del comercio electrónico, de seguridad de las transacciones electrónicas, de nuevas formas de contratación. La otra vertiente se refiere a la protección de los datos como *medio de protección de la persona* dirigido a salvaguardar uno de los principales derechos fundamentales, es decir, el derecho a la *vida privada*.

Por un lado, el debate se centra sobre la protección de los consumidores y de los contratantes frente a las nuevas formas de difusión y divulgación de los datos emitidos a través de las redes digitales, y por otro, se habla de la protección de las personas frente a la sociedad de la información⁶¹. Ambos modelos no son incompatibles, si bien parece lógico que, dado el carácter fundamental del derecho a la vida privada, se examinen con prioridad los instrumentos necesarios para otorgar al ciudadano, en cuanto persona (antes que como consumidor o contratante), la adecuada protección ante las nuevas tecnologías. Ello sin perder de vista que tal protección no se agota en la de los datos personales, ya que en la actual sociedad de la información, la noción de protección de la vida privada reviste un importante abanico de sectores. Para algunos, se trata del derecho a gozar de comunicaciones privadas, para otros, de no ser objeto de vigilancia o de hacer que sea respetado su cuerpo impidiendo la realización de determinadas prácticas. En definitiva, la protección de la vida privada debe ser explorada desde el ángulo de los derechos de la persona (Campuzano Tome, 2000: 55).

⁶¹ En este caso, nos referimos a la sociedad de la información, en lo que hace a la tendencia digital (internet, telecomunicaciones, etc.), con sus ventajas y riesgos. Es de señalar, que este término es interpretado de diversas formas como sociedad: del conocimiento, digital, de la comunicación, de la red, del ciberespacio, de telecomunicaciones, etc. (Ruiz de Querol y Buira, 2007: 18-21). La idea de la sociedad de la información tiene sus principales orígenes a partir de los 70's, a raíz de la revelación del proyecto, elaborado en 1973 por el Ministerio del Interior en Francia, de un sistema automatizado de ficheros administrativos y del repertorio de individuos (Safari), basado en la interconexión de cuatrocientos ficheros distintos a partir de un "identificador único", el número de afiliación a la Seguridad Social. El gobierno federal de Estados Unidos, presta atención al asunto de las telecomunicaciones y pone en circulación la expresión de "sociedad de la información" (en 1970, el presidente Richard Nixon cambia completamente el organigrama gubernamental de toma de decisiones en el ámbito de las tecnologías del cable, la informática y el satélite) (Mattelart, 2001: 118-121). Al respecto también se puede consultar Campuzano Tomé (2000: 17-49), Gómez Navajas (2005: 33-49), Veleiro (2008: 225 y ss.) y Del Peso Navarro (2003).

2. Definición formal

El derecho fundamental a la Protección de Datos Personales (PDP) es definido por la Sentencia 290/2000 del Tribunal Constitucional español, como aquel que garantiza a la persona un poder de control y disposición sobre sus datos personales. Dicho derecho confiere a su titular un haz de facultades que son elementos esenciales del derecho de PDP, integrado por la facultad que corresponde al afectado de consentir la recogida y el uso de sus datos personales, así como a conocer los mismos. Para hacer efectivo ese contenido, es incluido también, el derecho a ser informado de quién posee sus datos personales y con qué finalidad, así como el derecho a oponerse a esa posesión y uso exigiendo a quien corresponda, que ponga fin a la posesión y empleo de tales datos⁶².

En otras palabras, este nuevo derecho fundamental comprende un conjunto de derechos que la persona puede ejercer frente a quienes sean poseedores de ficheros públicos o privados, de saber el contenido, uso y destino de la información que se contenga en ellos. De suerte que, es sobre estos ficheros donde han de proyectarse, en última instancia, las medidas destinadas a la salvaguardia de este derecho fundamental, por parte de las Administraciones Públicas competentes⁶³.

Para una correcta protección de datos personales, se considera fundamental hacer referencia a la definición que, algunos ordenamientos, hacen del concepto de “datos personales” y la finalidad que persigue cada uno de estos instrumentos:

- a) Convenio No. 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.
 - Los datos de carácter personal con cualquier información relativa a una persona física identificada o identificable (persona concernida).

⁶² STC 290/2000, de 30 de noviembre, FJ 7.

⁶³ *Ídem*.

- Su finalidad es garantizar en el territorio de cada parte, a cualquier persona física sean cuales fueren su nacionalidad o su residencia, el respeto de sus derechos y libertades fundamentales, concretamente su derecho a la vida privada, con respecto al tratamiento automatizado de los datos de carácter personal correspondientes a dicha persona (protección de datos).
- b) Directiva 95/46/CE del Parlamento europeo y del Consejo, de 24 de octubre, 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.
- Los datos personales son toda información sobre una persona física identificada o identificable (el interesado); y que se considera 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.
 - Tiene por objeto que los Estados miembros garanticen, con arreglo a las disposiciones de esta 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.
- c) Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal (España).
- Los datos personales son cualquier información concerniente a personas físicas identificadas o identificables.
 - Su objeto es 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.

d) Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental, de 11 de junio de 2002 (México)⁶⁴.

- Los datos personales son cualquier información concerniente a una persona física identificada o identificable⁶⁵.
- Este ordenamiento es de orden público, y tiene como finalidad proveer lo necesario para garantizar el acceso de toda persona a la información en posesión de los Poderes de la Unión, los órganos constitucionales autónomos o con autonomía legal, y cualquier otra entidad federal.

e) Ley Federal de Protección de Datos Personales en posesión de los particulares, de 27 de abril de 2010 (México)⁶⁶.

- Los datos personales son cualquier información concerniente a una persona física identificada o identificable.
- Esta 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.

f) Ley 25.326, de protección de datos personales, sancionada el 4 de octubre de 2000 (Argentina)⁶⁷.

⁶⁴ A mayor abundamiento esta Ley ha sufrido una última reforma, la cual fue publicada en el Diario Oficial de la Federación el 5 de julio de 2010.

⁶⁵ Este concepto de datos personales sustituye al anterior, por la reforma que se hace a los arts. 3 y 33 de la Ley Federal de Transparencia y Acceso a la Información Pública, en la expedición de la Ley Federal de Protección de Datos Personales en posesión de los Particulares. El texto anterior definía a los datos personales, como la información concerniente a una persona física, identificada o identificable, entre otra, la relativa a su origen étnico o racial, o que esté referida a las características físicas, morales o emocionales, a su vida afectiva y familiar, domicilio, número telefónico, patrimonio, ideología y opiniones políticas, creencias o convicciones religiosas o filosóficas, los estados de salud físicos o mentales, las preferencias sexuales, u otras análogas que afecten su intimidad.

⁶⁶ Publicada en el Diario Oficial de la Federación el 5 de julio de 2010.

⁶⁷ Publicada en el Boletín Oficial el 2 de noviembre de 2000, actualizada en septiembre de 2007.

- Los datos personales es la información de cualquier tipo referida a personas físicas o de existencia ideal determinadas o determinables.
- 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.

g) Código de protección de datos personales, de 30 de junio de 2003 (Italia)⁶⁸.

- Datos personales son cualquier información relativa a una persona física, jurídica, entidad o asociación; identificados o identificables, incluso indirectamente, por referencia a cualquier otra información, incluido un número de identificación personal.
- Su finalidad es garantizar que el tratamiento de datos personales se desenvuelva en el respeto de los derechos y libertades fundamentales, así como de la dignidad humana, con especial referencia en la vida privada, la identidad personal y el derecho a la protección de datos personales.

3. Derecho autónomo o derecho derivado

Es importante contextualizar el derecho a la protección de datos personales como un derecho autónomo e independiente. En ocasiones, puede causar alguna confusión con el derecho a la privacidad o intimidad, ya que comparten rasgos particulares, como la protección a la vida privada de injerencias de terceros, por el uso indebido de la información personal. Una diferencia entre ambos derechos es que el derecho a la privacidad protege la vida privada en su ámbito más íntimo, como son las relaciones familiares; y el derecho a la protección de datos personales protege la información personal, ya sea privada o no, otorgando la facultad de controlar el uso, destino y permanencia de la misma

⁶⁸ *Codice in materia di protezione dei dati personali. Decreto legislativo 30 giugno 2003, n. 196.*

en un fichero, por ejemplo los datos profesionales en los registros de una asociación.

El derecho a la protección de datos personales, por su denominación, pareciera que sólo protege a los “datos”, pero no es así, este derecho protege a la persona de intromisiones ilegítimas en su vida privada, que se originan por el uso de los datos personales. La inclusión de este nuevo derecho es importante, ya que los datos aparentemente inocuos, acumulados con otros igualmente inofensivos, podrían arrojar un perfil personal⁶⁹, y fácilmente se podría identificar a un individuo. Así, las personas se vuelven altamente vulnerables, ante la cantidad de información que las bases de datos almacenan.

Actualmente, la doctrina ha aclarado y agotado la posición de que el derecho a la autodeterminación informativa (protección de datos personales) forme parte del derecho a la intimidad personal o familiar. Es decir -y como se detallará posteriormente-, si bien este derecho surge a partir del derecho a la privacidad, su evolución ha sido tal, que hoy en día, tiene una mayor amplitud, lo que no le permite seguir en un ámbito tan delimitado como el derecho a la intimidad.

La intimidad y el derecho a la protección de datos personales (autodeterminación informativa), son derechos fundamentales directamente ligados a la dignidad humana. El derecho a la intimidad se caracteriza por un eminente contenido negativo para salvaguardar del conocimiento ajeno una parte de nuestra vida personal y familiar, es decir, aquella que deseamos tener en el lado más reservado o secreto. El derecho a la autodeterminación informativa, por su parte, tiene un contenido diferente, su ámbito es más amplio y los elementos que lo componen más complejos. El tratamiento de la información personal

⁶⁹ Con relación a los perfiles personales Garriga Domínguez (2004: 25) dice que los datos pueden utilizarse de forma más o menos aislada, o bien, reunirse y confrontarse. Esta interrelación de las informaciones personales permitirá la obtención del perfil de cualquiera y servirá para que se adopten decisiones que le afecten sin que las personas *sean tenidas en cuenta ni consultadas*. El perfil, ya sea del consumidor, del internauta, del asegurado, del empleado, del estudiante o del profesor, económico, ideológico o sexual, permite obtener una *radiografía* de toda o de parte de su vida, así como prever –o al menos intuir- sus reacción y comportamientos futuros. El tratamiento de los datos personales *hace posible una vigilancia de hecho de la vida cotidiana del individuo*, al permitir el registro de una serie de datos que separadamente carecen de importancia, pero que adecuadamente relacionados permiten obtener el perfil de una persona.

puede, pero no tiene por qué, afectar a informaciones íntimas o secretas que son el objeto de protección del derecho a la intimidad. De la misma forma, los datos personales informatizados no tienen necesariamente que precipitar un retrato personal que implique una valoración peyorativa u ofensiva de un individuo y que atente contra su buen nombre o fama (Garriga Domínguez, 2004: 22).

Al respecto de la configuración de un derecho autónomo, distinto al derecho a la intimidad, el voto particular del Magistrado Manuel Jiménez de Parga y Cabrera, en la Sentencia del Tribunal Constitucional de España número 290/2000 (al que se adhiere el Magistrado Rafael de Mendizábal Allende), dice que: “como ya expuse en las deliberaciones del Pleno, debió afirmarse de modo explícito, en la argumentación de ella, que nuestro Tribunal reconoce y protege ahora un derecho fundamental, el *derecho de libertad informática*, que no figura en la Tabla del texto de 1978”. Voto particular que amén de la importancia que tiene de cara a subrayar el nacimiento de un nuevo derecho fundamental de creación jurisprudencial, el cual es el derecho fundamental a la protección de datos personales o libertad informática⁷⁰, abre las puertas al reconocimiento de nuevos derechos fundamentales por la Jurisprudencia del Tribunal Constitucional⁷¹.

Los derechos fundamentales de creación jurisprudencial, son aquellos de nueva concepción “no escritos” y considerados de la última tendencia de derechos. Por su momento de aparición, han de ser tutelados por la jurisprudencia, al no estar contemplados en las Constituciones, las cuales proporcionan al intérprete un punto de apoyo, unas palabras (escasas a veces, lapidarias) sobre las que hay que efectuar, mediante una actividad creadora, la construcción de un derecho⁷².

⁷⁰ El voto particular hace derivar la libertad informática no sólo del art. 18.4 CE, sino sobre todo del art. 10.1 CE, en cuanto el reconocimiento del citado derecho es necesario para garantizar la dignidad de la persona, los derechos inviolables que le son inherentes y el libre desarrollo de la personalidad.

⁷¹ Véase también a Corripio Gil-Delgado y Marroig Pol (2001: 45-81) sobre el camino hacia la construcción de un derecho fundamental a la protección de datos personales.

⁷² Cuestión, ésta, de enorme interés que sería materia suficiente para una monografía, sin embargo, la misma no es objeto de estudio en el presente trabajo. Al respecto sobre el derecho fundamental a la protección de datos personales como construcción jurisprudencial véase a Palomar Olmeda (2007: 14-15).

4. El origen de la protección de datos personales. Privacidad y/o intimidad.

El derecho a la *privacidad* es aquel que protege física y psicológicamente al individuo de intromisiones no deseadas por éste, provenientes de terceros. La privacidad constituye un ámbito de difícil delimitación, por lo que queda sujeta a las disposiciones normativas existentes y al voto de confianza que los ciudadanos hagan a sus Tribunales, quienes al estudiar cada caso en concreto, habrán de decidir además de lo conducente por la ley, lo que proceda según las circunstancias particulares.

Se dice que la privacidad y la intimidad, constituyen conceptos que si bien son parecidos, no son idénticos dado su ámbito de protección, del cual se deduce que la privacidad sería el género y la intimidad la especie⁷³. La Real Academia Española (RAE) nos dice que la *privacidad* es el ámbito de la vida privada que se tiene derecho a proteger de cualquier intromisión; mientras que la *intimidad* es aquella zona espiritual íntima y reservada de una persona o de un grupo, especialmente de una familia.

Con relación a las definiciones que la RAE proporciona, la *privacidad* es constituida –valga la redundancia– por la vida privada, y es sabido que, ésta comprende el desenvolvimiento de la actividad de la persona, en sus dos facetas: la *externa* y la *interna*. La primera, se refiere al comportamiento del individuo, que ya sea de forma solitaria o grupal, tiene una proyección física al exterior, por ejemplo, ir al cine solo o acompañado (por amigos, familia, etc.). La segunda, se puede situar en el campo del pensamiento, las ideas y los sentimientos, por ejemplo, el que cada quien tenga la ideología política, religiosa y moral que así desee.

La *intimidad* –según la definición de la RAE– es la zona espiritual, y por lo tanto, es la zona emocional, sensible e inmaterial de la persona, misma que conduce hacia las ideas y pensamientos, los cuales se ocupan de diferentes ámbitos como el familiar, el social, el laboral, etc. Estas ideas y pensamientos, una vez exteriorizados en la forma que se decida y hacia quienes se elija,

⁷³ Enciclopedia Jurídica Omeba. Versión Digital. Argentina, 2005. p. 28. Refiere que todo lo íntimo es necesariamente privado, pero no todo lo privado es necesariamente íntimo.

regresamos hacia el primer concepto, es decir, el de la vida privada, por ejemplo el simpatizar con las ideas de alguna religión y con posterioridad acudir frecuentemente al templo.

Así mismo, cabe destacar la diferencia que existe entre un secreto y la intimidad, Herrán (1998: 15) nos dice que el primero se caracteriza por el deber de ocultamiento y nace de la idea de compartir, de hacer cómplices a los demás de nuestras vivencias y sentimientos; mientras que la intimidad esta próxima a la idea de reserva, de disfrute interior de la propia existencia.

En este orden de ideas y con relación a la *intimidad* (sin exteriorización), es difícil pensar que pueda ser controlada e incluso protegida eficazmente por algo o por alguien. Por ello, hoy en día resulta imposible la existencia de una “policía del pensamiento”⁷⁴, como aquella que refiere George Orwell en su obra “1984”. Además que en la actualidad los diferentes ordenamientos jurídicos internacionales protectores de los derechos humanos, reconocen la libertad de pensamiento, conciencia y religión. La intimidad, como la idea de pensamiento y opiniones, se encuentra protegida desde la Declaración de los Derechos del Hombre y del Ciudadano de 1789, producto de la Revolución Francesa; así como por los instrumentos nacidos con posterioridad, como la Declaración Universal de los Derechos Humanos de 1948, producto de la vergonzosa historia de la humanidad, como lo es la segunda guerra mundial y los campos de concentración del holocausto⁷⁵.

En el caso español, la LO 5/1992, de 29 de octubre relativa a la Regulación del Tratamiento Automatizado de los Datos de Carácter Personal

⁷⁴ La obra *1984* de George Orwell, es una novela de ideología política de sucesos que acontecían a mediados del siglo XX. Una de las figuras creadas dentro de la novela es la “*policía del pensamiento*”, la cual se encargaba de vigilar al ciudadano precisamente en la forma más privada de la persona, es decir, su mente, pero siempre y cuando éstas fueran exteriorizadas por actos tales como gestos, miradas, movimientos del cuerpo, etc.

⁷⁵ “Derecho al pensamiento es el derecho fundamental que tiene todo ser humano (a) a configurar las propias ideas, opiniones, creencias o convicciones; (b) y a expresarlas por cualquier medio; (c) y a difundirlas por los medios masivos; (d) y a obrar con libertad interior en el cumplimiento del propio deber, especialmente del deber religioso; (e) y a contribuir con todo ello, a la configuración de una verdad comunitaria u opinión pública, pero permaneciendo exento frente a ella, para discutirla, criticarla o modificarla”, este derecho se encuentra de modo directo en los arts. 16.1 y 20.1 CE; e indirectamente en los arts. 14, 16.2, 20.1, 55.1 y 71.1 CE (Puy, 1985b: 167-169).

(LORTAD⁷⁶) –actualmente derogada por la LOPD 15/1999, de 13 de diciembre⁷⁷- contenía en su preámbulo las motivaciones que la originaban, así como la alusión de varios conceptos, entre los que destaca la diferencia que hace entre privacidad e intimidad⁷⁸.

En dicho preámbulo, el legislador español distingue entre los conceptos de privacidad e intimidad, y refiere que la primera es más amplia que la segunda. Explica, por su parte, que la intimidad es la faceta reservada de la vida, que abarca no solo los sentimientos, sino también, el domicilio, las comunicaciones, etc. Mientras que la privacidad, constituye un conjunto más amplio de facetas de la personalidad del individuo que, coherentemente enlazadas entre sí, arrojan un retrato de la personalidad, el cual cada individuo tiene derecho a mantener reservado.

Así pues, los datos personales son englobados por el legislador en el ámbito de la privacidad y no así en el de la intimidad. Los cataloga de ésta manera, partiendo del entendimiento de que aquellos, aparentemente inocuos y acumulados, nos arrojan el retrato de la persona, y se constituyen en eslabones de una cadena que generan un todo final⁷⁹ (Rebollo Delgado, 2006: 117), los cuales

⁷⁶ BOE 31/10/1992, n. 262.

⁷⁷ BOE 14/12/1999, n. 298.

⁷⁸ La redacción literal es la siguiente: “El progresivo desarrollo de las técnicas de recolección y almacenamiento de datos y de acceso a los mismos ha expuesto a la privacidad, en efecto, a una amenaza potencial antes desconocida. Nótese que se habla de la privacidad y no de la intimidad: Aquella es más amplia que ésta, pues en tanto la intimidad protege la esfera en que se desarrollan las facetas más singularmente reservadas de la vida de la persona -el domicilio donde realiza su vida cotidiana, las comunicaciones en las que expresa sus sentimientos, por ejemplo-, la privacidad constituye un conjunto, más amplio, más global, de facetas de su personalidad que, aisladamente consideradas, pueden carecer de significación intrínseca pero que, coherentemente enlazadas entre sí, arrojan como precipitado un retrato de la personalidad del individuo que éste tiene derecho a mantener reservado. Y si la intimidad, en sentido estricto, está suficientemente protegida por las previsiones de los tres primeros párrafos del artículo 18 de la Constitución y por las leyes que los desarrollan, la privacidad puede resultar menoscabada por la utilización de las tecnologías informáticas de tan reciente desarrollo”.

⁷⁹ Se puede decir que, la privacidad de la que habla el legislador en esta ley, son los llamados *perfiles personales*, que constituyen un ataque tan radical a la intimidad y a la propia imagen. Al respecto, dice Garriga Domínguez (2004: 26) que: “la obtención del *perfil* supone establecer una correlación entre la posesión de determinadas características (desunión familiar, fracaso escolar, estilos de vida, hábitos de consumo, etc.) y comportamientos concretos. Es decir, implica incardinar a una persona, en función del resultado del tratamiento informatizado de sus datos, en determinado grupo al que se le atribuyen unos determinados comportamientos futuros, cuya utilización en la toma de decisiones, que afecten a los sujetos de tales operaciones, pueden suponer una valorización desfavorable de sus rasgos y características personales, lo que al final supondría su discriminación para la obtención de un crédito, de un empleo, de un ascenso, etc., o

mal utilizados producirán, sin lugar a dudas, una vulneración de la intimidad⁸⁰ (Amoroso Fernández, 1991: 42).

En este sentido, por lo que hace a la diferenciación de *privacy* y *riservatezza* –entendida como la intimidad en el caso español- Serrano Pérez (2003: 40) aclara que puede ser que en algún punto de su contenido ambos términos se aproximen bastante, puesto que ambas figuras surgen para frenar injerencias no consentidas, esto es, con un sentido de defensa; pero que la evolución de ambos vocablos no ha transcurrido de forma paralela, advirtiéndose una mayor amplitud en el primero que en el segundo. Por su parte, Cifuentes (2007: 73) dice que no hay diferenciación que hacer de estos dos términos conceptuales (intimidad y vida privada).

Es de considerar que las facetas personales del individuo no se pueden categorizar en dos grandes grupos, tales como la intimidad y la privacidad, los cuales no se llegan a delimitar apropiadamente, por el solo pudor del uso que sugiere la palabra intimidad. Como se ha visto, la definición de ambos conceptos es cercana entre sí, aunque algunos consideren que la intimidad es más profunda y que la privacidad es más amplia por el cúmulo de facetas de la vida que contempla.

Ahora bien, y haciendo más extensa la discusión en relación a los términos de privacidad e intimidad, como adjetivos para calificar a las facetas de la vida, es decir como parte de la vida privada o vida íntima; también se podría utilizar el término “personal”. La vida personal, es una expresión opuesta a vida colectiva, así como privado a público, e íntimo a externo. Pero claro, el vocablo “personal”, resulta ser un concepto que al final connota lo mismo que los dos conceptos que se han venido analizando, porque hace referencia a la persona en lo particular. Por tal motivo, hoy considero que, tanto el concepto de privacidad y de intimidad resultan ser lo mismo, aclarando que el concepto de privacidad es un

la harían acreedora de una *especial vigilancia y control* al encajar su radiografía informática en el perfil del posible delincuente, terrorista o disidente de la ideología mayoritaria”.

⁸⁰ Como lo indica la autora en su artículo, es cierto que no son los grandes sistemas de información los que afectan la vida privada, sino la manipulación y especulación o el consentimiento de ello, por parte de individuos poco conscientes e irresponsables, de los datos que dichos sistemas contienen.

anglicismo proveniente de la palabra “*privacy*” (Warren y Brandeis, 1995: 11), misma que como también se ha dicho, resulta ser la más usada y aceptada, incluso por el diccionario de la Real Academia Española⁸¹. Por ello, en lo subsecuente y para efectos prácticos se hará referencia, en la mayor parte de ésta investigación, a la vida privada y al derecho a la privacidad, sin perjuicio de utilizar el término de la intimidad como sinónimo.

Por último, no quisiera terminar este apartado sin antes referir aquellas palabras del maestro Eduardo Novoa cuando dice que la verdad es que el derecho a la vida privada o el derecho a la intimidad, han alcanzado hoy un significado jurídico especial que las explicaciones lexicológicas no agotan, y que para comprender ese significado en forma más exacta hemos de esperar hasta profundizar más en el concepto jurídico (Novoa Monreal, 2001: 31).

5. Bien jurídico protegido

El derecho a la intimidad normalmente conlleva el poder jurídico de rechazar intromisiones ilegítimas en la esfera protegida y, correlativamente, decidir libremente y dentro de ella la propia conducta, estamos pues frente a un típico derecho de defensa. Sin embargo, la técnica del derecho a la protección de datos personales es más compleja y amplia, ya que por un lado combina poderes del individuo frente a terceros (límites y prohibiciones) con diversas garantías instrumentales y; por otro lado, los datos que se protegen no tienen por qué ser íntimos, basta con que sean personales, aun cuando parezcan inofensivos (Ruiz Miguel, 2004: 241).

Por su parte, Ricard Martínez Martínez (2004: 47) señala que el bien protegido por el derecho a la vida privada no es otro que la información personal, es más, cualquier tipo de información personal susceptible de revelar aspectos privados del individuo, ya sea por sí sola, o mediante su consideración conjunta con otras informaciones o gracias a la realización de algún tipo de tratamiento.

⁸¹ Con relación a la evolución del contenido de los términos de intimidad y vida privada véase a Martínez Martínez (2004: 27-44).

Sin embargo, es importante aclarar que el derecho a la protección de datos personales, no protege a los datos *per se*, sino al titular de los mismos, ya que la información por sí sola no implica un peligro, sino la asociación de esta con una determinada persona.

6. Habeas data

El *hábeas data*, como se ha dicho antes, es un derecho de reciente creación, y por lo tanto, es una garantía constitucional moderna, aunque su denominación sea, mitad en latín y mitad en inglés. Su nombre se ha tomado parcialmente del antiguo instituto del *hábeas corpus*, en el cual el primer vocablo significa “conserva o guarda tu...”, y del inglés “*data*”, sustantivo plural que significa “información o datos”. Por lo tanto, en una traducción literal sería “conserva o guarda tus datos” (Ekmekdjian y Pizzolo, 1996: 1).

La Constitución brasileña de 1988 es la primera en introducir la acción de *Hábeas Data*, cuya naturaleza es la de una acción destinada a garantizar el derecho de los ciudadanos al acceso y la rectificación de sus datos personales en posesión de terceros. Esta figura brasileña influyó en su entorno geográfico, de tal manera que se encuentra hoy en países como: Argentina, Colombia, Ecuador, Guatemala, Paraguay, Perú, Uruguay y Venezuela⁸². La presencia de esta acción en varios ordenamientos latinoamericanos está vinculada a razones de orden geopolítico. Un instituto de este tipo tenía una especial razón de ser en sociedades recién salidas de regímenes militares, como era el caso de diversos países latinoamericanos a partir de la década de 1980, en los cuales persistía el trauma causado por el uso autoritario de la información como instrumento de represión política (por ejemplo la información contenida en registros policiales a los que antes no se tenía acceso). Esta herramienta fue concebida para permitir al ciudadano conocer directamente y, en caso necesario, rectificar las informaciones que sobre él se almacenan en bases de datos (Agencia Española de Protección de Datos, 2011: 5-6).

⁸² En 1988 Brasil es el primero en introducir el *hábeas data* en su Constitución, en 1999 Chile es el primero en emitir una ley de protección de datos, mientras que Argentina con su ley del 2000 es el que más ha desarrollado el derecho en Latinoamérica (Agencia Española de Protección de Datos Personales, 2011: 12).

La acción de *hábeas data* se define como “el derecho que asiste a toda persona –identificada o identificable- a solicitar judicialmente la exhibición de los registros –públicos o privados- en los cuales están incluidos sus datos personales o los de su grupo familiar, para tomar conocimiento de su exactitud; a requerir la rectificación, la supresión de datos inexactos u obsoletos o que impliquen discriminación (...). Esta herramienta tiende a proteger a la persona contra *calificaciones sospechosas* incluidas en registros (especialmente estatales, aunque también pueden serlo privados), que –sin darle derecho de contradecirlas- pueden llegar a perjudicarlo de cualquier modo” (Ekmekdjian y Pizzolo, 1996: 1-2). Es de destacar, nuevamente, que la protección de datos no ha sido creada para proteger a los datos *per se*, sino a las personas titulares de estos, para resguardarlas de arbitrariedades por parte del manejo que de dicha información personal hagan los responsables de los bancos de datos.

El *hábeas data* es una garantía especial que protege –fundamentalmente- el derecho a la intimidad (o privacidad), el cual deriva del derecho a la dignidad. Actualmente, el concepto de *hábeas data* es otra manera de denominar el derecho de autodeterminación informativa o el derecho a la protección de datos personales. Sin embargo, y como se ha podido ver por la naturaleza de su origen, son diferentes por la autoridad garante. El *hábeas data*, refiere el ejercicio del derecho frente a la autoridad judicial, a través del proceso respectivo; mientras que la autodeterminación informativa o protección de datos es frente a una Autoridad que forma parte de la Administración Pública, cuyas resoluciones pueden ser recurridas judicialmente.

7. Intimidad

La intimidad es considerada por el TCE como un derecho desvinculado de una óptica patrimonialista y así aparece ligado a la esfera de la personalidad individual (Garriga Domínguez, 2004: 21). El derecho fundamental a la intimidad 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”⁸³.

La STC 142/1993 refiere que el “atributo más importante de la intimidad, como núcleo central de la personalidad, es la facultad de exclusión de los demás, de abstención de injerencias por parte de otro, tanto en lo que se refiere a la toma de conocimientos intrusiva, como a la divulgación ilegítima de esos datos”⁸⁴.

El art. 18.1 CE garantiza el derecho a la intimidad que comprende, entre otros, los derechos a la intimidad personal y a la propia imagen, que forman parte de los bienes de la personalidad pertenecientes al ámbito de la vida privada. La STC 170/1987 refiere que estos derechos salvaguardan un espacio de intimidad personal y familiar, que se sustrae de intromisiones extrañas⁸⁵. En este ámbito de la intimidad, reviste singular importancia la necesaria protección del derecho a la propia imagen frente al creciente desarrollo de los medios y procedimientos de captación, divulgación y difusión de la misma, así como de datos y circunstancias pertenecientes a la intimidad que garantiza este precepto.

8. Derecho a la información

El derecho a la información, es un derecho consagrado en el art. 19 de la Declaración Universal de Derechos Humanos (DUDH) de 10 de diciembre de 1948, el cual a la letra dice que “todo individuo tiene derecho a la libertad de opinión y de expresión; este derecho incluye el de no ser molestado a causa de sus opiniones, el de investigar y recibir informaciones y opiniones, y el de difundirlas, sin limitación de fronteras, por cualquier medio de expresión”. En este derecho se encuentran incluidas la libertad de opinión, de expresión y de información⁸⁶. Este derecho ha sido estudiado en las últimas décadas por muchos

⁸³ STC 231/1988, de 2 de diciembre, FJ 3.

⁸⁴ STC 142/1993, de 22 de abril, FJ 7.

⁸⁵ STC 170/1987, de 30 de octubre, FJ 4.

⁸⁶ Desantes Guanter (1976: 25-26) dice que la información nunca podrá tener como destinataria la masa, ya que, o se dirige al hombre individualizado o al hombre en colectividad, lo que cualitativamente es lo mismo. Si se dirige al hombre en colectividad está cumpliendo una función pública, pero respetando la personalidad de cada destinatario, aunque éste sea desconocido, indeterminado y aun indeterminable.

autores, a continuación precisaremos algunos, además de lo que en el TCE ha puntualizado con relación al derecho al honor y la intimidad.

Martí Capitanachi (2007: 98) refiere que, el derecho a la información surge como una reacción a los regímenes totalitarios, que privilegiaban la información oficial, en los cuales los receptores no tenían opción de contrarrestar las noticias o informaciones gubernamentales en otros medios de difusión, por lo que los derechos de los receptores se incluyen de manera expresa⁸⁷. Así, con posterioridad a la DUDH, surgen distintos instrumentos internacionales que incluyen este derecho, tales como el Pacto Internacional de los Derechos Civiles y Políticos de 1966 y la Convención Americana de Derechos Humanos de 1969.

Desantes Guanter (1974: 33) dice que el derecho a la información se debe entender como un derecho del ciudadano correlativo al derecho a la participación y, en consecuencia, sin más limitaciones que las que a ésta se le impongan por razones verdaderamente excepcionales y con todo el alcance activo de la participación.

Para Nogueira Alcalá (2003: 26) la libertad de información comprende el derecho a investigar y acceder a las fuentes de información, a transmitir la información de cualquier forma y a través de cualquier medio sin censura ni restricciones preventivas y el derecho a recibir, seleccionar y rectificar las informaciones difundidas, debiendo el Estado, sus agentes y órganos respetar tales derechos, garantizarlos, como promoverlos, contribuyendo al desarrollo del pluralismo informativo, previniendo, la existencia de censuras directas o indirectas, administrando con transparencia, racionalidad y justicia el acceso a las frecuencias radioeléctricas, impidiendo la existencia de monopolios u oligopolios respecto de los medios o insumos necesarios para producir la información escrita, por cable o de cualquier otro modo o medio, como por último, impidiendo la

⁸⁷ El derecho a la información garantiza dos aspectos, por un lado el derecho a informar y por otro el derecho a ser informado, en este último se encuentran además el derecho de acceso a la información pública y el derecho a la información privada (Ríos Estavillos, 2005: 125).

constitución de monopolios públicos o privados sobre todo los tipos de medios de comunicación social⁸⁸.

Para Villanueva el derecho a la información se trata de una rama de formación de la ciencia del derecho en busca de su autonomía respecto de las ramas clásicas de la ciencia jurídica, que podría definirse como la rama del derecho público que tiene por objeto el estudio de las normas jurídicas que regulan, en *lato sensu*, las relaciones entre Estado, medios y sociedad, así como, en *strictu sensu*, los alcances y los límites del ejercicio de las libertades de expresión y de información y el derecho a la información a través de cualquier medio (Villanueva, 2003: XVIII, 2006a: 10; Nava Gomar, Luna Pla y Villanueva, 2006: 8)⁸⁹.

En *strictu sensu*, el derecho a la información, se refiere además a la “prerrogativa de la persona para examinar datos, registros y todo tipo de informaciones en poder de entidades públicas y empresas privadas que ejercen gasto público, cumplen funciones de autoridad o están previstas por las disposiciones legales como sujetos obligados por razones de interés público, con las excepciones taxativas que establezca la ley en una sociedad democrática” (Caballero Juárez et al., 2006: 11). De esta manera, refiere el autor que el *lato sensu* es el sentido genérico con el que se define el derecho a la información,

⁸⁸ El derecho de acceso a la información, se entiende bajo la estructura de principio, es decir, de un mandato de optimización que obliga algo a ser realizado en la máxima medida posible, de acuerdo a las posibilidades fácticas y jurídicas. A diferencia de las reglas, por tanto, se aplica de manera gradual y la colisión entre principios se resuelve a través de la ponderación (García P. y Contreras, 2009: 142-143).

⁸⁹ Villanueva (2003: XVII) está de acuerdo con la definición que proporciona la Declaración Universal de Derechos Humanos, con relación al derecho a la información, que es la garantía fundamental que toda persona posee a: atraerse información, a informar y a ser informada. Asimismo, el autor no explica las facultades de cada una de estas tres facetas. El derecho a atraerse información incluye las facultades de a) acceso a los archivos, registros y documentos públicos y, b) la decisión de que medio se lee, se escucha o se contempla. El derecho a informar incluye las a) libertades de expresión y de imprenta y, b) el de constitución de sociedades y empresas informativas. Y el derecho a ser informado incluye las facultades de a) recibir información objetiva y oportuna, b) la cual debe de ser completa, es decir, el derecho a enterarse de todas las noticias y, c) con carácter universal, o sea, que la información es para todas las personas sin exclusión alguna.

mientras que en el *strictu sensu* se estaría acuñando lo que se conoce como el *derecho de acceso a la información pública*⁹⁰.

El Tribunal Constitucional español ha dicho, que dada la función institucional del derecho a la información, cuando se produzca una colisión de la libertad de información con el derecho a la intimidad y al honor, aquella goza en general, de una posición preferente y las restricciones que de dicho conflicto puedan derivarse a la libertad de información deben interpretarse de tal modo que el contenido fundamental del derecho a la información no resulte, dada su jerarquía institucional, desnaturalizado ni incorrectamente relativizado (SSTC 106/1986, de 24 de julio, y 159/1986, de 16 de diciembre, entre otras). Esta postura del Tribunal, puede ser discutible, porque da *a priori* otorga más valor a un derecho que a otro, sin entrar en la debida ponderación de derechos atendiendo al caso particular. Es interesante, que en el proyecto de Ley de Transparencia española, el art. 12.4 hace una mención muy particular de los criterios a seguir en la ponderación del derecho de acceso a la información y el derecho de protección de datos personales⁹¹.

Por otro lado, es de señalar que para el caso mexicano y como se verá en el apartado correspondiente a México, este cuenta desde el 2002 con la Ley Federal de transparencia y acceso a la información pública gubernamental. Y

⁹⁰ “El derecho de acceso a la información tiene como propósito coadyuvar con la sociedad en su conjunto a fin de que el derecho a saber pueda ser vigente y, por supuesto, eficaz. Por esta razón, el otorgamiento de información no debe depender de la existencia de un interés específico en la información. Este principio es esencialmente una cláusula de no discriminación. Y con él se busca asegurar que la información sea dada a todos los que la busquen, con la misma base y el mismo grado” (Villanueva, 2006b: 11).

⁹¹ El proyecto de Ley de transparencia, acceso a la información pública y buen gobierno en España, aprobado por el Consejo de Ministros el 17 de julio de 2012, en su art. 12.4 establece lo siguiente: Cuando la información solicitada no contuviera datos especialmente protegidos, el órgano al que se dirija la solicitud concederá el acceso previa ponderación suficientemente razonada del interés público en la divulgación de la información y los derechos de los afectados cuyos datos aparezcan en la información solicitada, en particular su derecho fundamental a la protección de datos de carácter personal. Para la realización de la citada ponderación, el órgano tomará particularmente en consideración los siguientes criterios: a) El menor perjuicio a los afectados derivado del transcurso de los plazos establecidos en el artículo 57 de la Ley 16/1985, de 25 de junio, del Patrimonio Histórico Español; b) La justificación por los solicitantes de su petición en el ejercicio de un derecho o el hecho de que tengan la condición de investigadores y motiven el acceso en fines históricos, científicos o estadísticos; c) El menor perjuicio de los derechos de los afectados en caso de que los documentos únicamente contuviesen datos de carácter meramente identificativo de aquellos; y d) La mayor garantía de los derechos de los afectados en caso de que los datos contenidos en el documento puedan afectar a su intimidad o a su seguridad.

desde el 2010 con la Ley Federal de protección de datos personales en posesión de particulares. Por lo que en los subsecuentes años, será interesante observar la conducta de ambos derechos y la tendencia que marcaran los tribunales en lo que hace a la ponderación del derecho de información y el de protección de datos personales.

9. Inserciones constitucionales de relevancia

En este espacio, se verá cómo el derecho a la protección de datos personales ha tenido su origen en Portugal, Alemania, Francia y además de –por ahora- hacer una breve referencia del caso español, ya que a España le dedicamos un apartado más amplio de nuestro estudio. Ahora bien, y sin la intención de agotar el tema en cada uno de estos países, se hará una breve descripción de lo dispuesto por la Constitución, la ley de la materia y a la institución encargada de velar por el debido cumplimiento del respeto de este derecho.

Se describe lo dispuesto por los artículos constitucionales que tienen que ver con el derecho a la privacidad, libertades informáticas, protección de datos y dignidad de la personas, por su importancia para este estudio.

Se han seleccionado específicamente los casos de Portugal, Francia, Alemania y España por ser los más significativos en el origen y evolución del derecho a la protección de datos personales en Europa y por la importancia que este derecho tiene en sus constituciones. Portugal es el primer país que introdujo la protección de este derecho en su Constitución, en Alemania nace el derecho a la autodeterminación informativa (por ello es que se dice que es de creación europea), Francia ha mostrado un avance significativo a la hora de legislar en la materia, mientras que España por sus vínculos históricos con Latinoamérica es la que más ha contribuido e influenciado los nuevos ordenamientos de protección de datos personales en América Latina.

9.1 Portugal

A. Constitución

La Constitución portuguesa de 2 de Abril de 1976, contiene el primer antecedente constitucional que expresamente regula el derecho a la protección de datos personales (art. 35). Así mismo, existe en dicho ordenamiento la garantía de la dignidad humana (art. 26) y del derecho a la privacidad reflejado en el derecho de la inviolabilidad del domicilio y de la correspondencia (art. 34).

El art. 26 de la Constitución portuguesa reconoce el derecho al buen nombre y reputación, a la imagen, a la palabra, a la reserva de la intimidad de la vida privada y familiar. En el segundo párrafo, establece las garantías efectivas contra la utilización abusiva, o contraria a la dignidad humana, de informaciones relativas a las personas y a las familias. Y en el tercero, refiere que la ley garantizará la dignidad personal y la identidad genética del ser humano, especialmente en la creación, desarrollo y utilización de la tecnología y en la experimentación científica. La mención anterior de este artículo previendo el manejo de la tecnología, es muestra del avance del legislador portugués en la elaboración de la norma adecuándola a la realidad y al futuro de la sociedad⁹².

El art. 34 de la Constitución de Portugal establece la inviolabilidad del domicilio, la correspondencia y de otros medios de comunicación privada. La mención de “otros medios de comunicación” continúa con la evidente línea de máxima previsión de las nuevas formas de comunicación de la sociedad, principalmente, a través de internet⁹³.

⁹² Artículo 26 (Otros derechos personales). 1. Se reconoce a todos el derecho a la identidad personal, al desarrollo de la personalidad, a la capacidad civil, a la ciudadanía, al buen nombre y reputación, a la imagen, a la palabra, a la reserva de la intimidad de la vida privada y familiar y a la protección legal contra cualesquiera formas de discriminación; 2. La ley establecerá garantías efectivas contra la utilización abusiva, o contraria a la dignidad humana, de informaciones relativas a las personas y a las familias; 3. La ley garantizará la dignidad personal y la identidad genética del ser humano, especialmente en la creación, desarrollo y utilización de la tecnología y en la experimentación científica; y 4. La privación de la ciudadanía y las restricciones a la capacidad civil sólo pueden efectuarse en los casos y en los términos previstos por la ley, no pudiendo tener como fundamento motivos políticos. Este último es el artículo vigente, que antes se encontraba redactado así: Art. 33 (Derecho a la identidad, buen nombre e intimidad) 1. A todos es reconocido el derecho a la identidad personal, al buen nombre y reputación, y a la reserva de la intimidad de la vida privada y familiar. 2. La ley establecerá garantías efectivas contra la utilización abusiva o contraria a la dignidad humana, de información relativa a las personas y familia.

⁹³ Artículo 34 (De la inviolabilidad del domicilio y de la correspondencia). 1. El domicilio y el secreto de la correspondencia y de otros medios de comunicación privada son inviolables; 2. La entrada en el domicilio de los ciudadanos, contra su voluntad, sólo puede ser ordenada por la autoridad judicial competente, en los casos y según las formas previstas por la ley; 3. Nadie puede

Si bien los artículos anteriores regulaban las comunicaciones, el uso de la tecnología, la vida privada y familiar, etc. El art. 35 de esta Constitución es el más significativo para nuestra investigación porque regula la utilización de la informática, en beneficio de los ciudadanos como usuarios de ella⁹⁴. Se destaca la acertada decisión del legislador portugués en incluir dicha garantía.

Así, la redacción actual del art. 35 constitucional⁹⁵, relativo a la *Utilización de la informática*, establece que todos los ciudadanos tienen derecho a acceder a los datos informatizados que les conciernan, pudiendo exigir su rectificación y actualización, así como el derecho a conocer la finalidad a que se destinan, en los términos que establezca la ley. Asimismo, deriva a la Ley de la materia en lo que hace al desarrollo del derecho, y a su garantía a través de una autoridad administrativa independiente.

El propio texto constitucional prohíbe la utilización de la informática para el tratamiento de datos relativos a convicciones filosóficas o políticas, afiliación a

entrar durante la noche en el domicilio de ninguna persona sin su consentimiento; y 4. Se prohíbe toda injerencia de las autoridades públicas en la correspondencia, en las telecomunicaciones y en los demás medios de comunicación, salvo en los casos previstos en la ley en materia de procedimiento penal. El artículo continua casi intacto respecto de su redacción de 1976, salvo por el último número 4.

⁹⁴ El texto original del artículo se encontraba redactado así: Artículo 35 (Utilización de la informática) 1. Todos los ciudadanos tienen el derecho de tomar conocimiento de que consta en registros mecanográficos de su persona y de los fines a que se destina tal información, pudiendo exigir la rectificación de sus datos y de su actualización. 2. La informática no puede ser usada para el tratamiento de datos referentes a convicciones políticas, de la fe religiosa o vida privada, salvo cuando se trate del procesamiento de datos no identificables para fines estadísticos. 3. Está prohibida la atribución de un número nacional único a los ciudadanos. Cualquier error en la traducción es responsabilidad de la autora de esta tesis. Con relación a este dispositivo también se puede consultar a Soares Martínez (1978: 6).

⁹⁵ Artículo 35. Utilización de la informática. 1. Todos los ciudadanos tienen derecho a acceder a los datos informatizados que les conciernan, pudiendo exigir su rectificación y actualización, así como el derecho a conocer la finalidad a que se destinan, en los términos que establezca la ley; 2. La ley define el concepto de datos personales, así como las condiciones aplicables a su tratamiento automatizado, conexión, transmisión y utilización, y garantiza su protección, especialmente a través de una entidad administrativa independiente; 3. La informática no puede ser utilizada para el tratamiento de datos relativos a convicciones filosóficas o políticas, afiliación a partidos o sindicatos, confesión religiosa, vida privada y origen étnico, salvo con el consentimiento expreso del titular, autorización prevista por la ley con garantías de no discriminación o para procesamiento de datos estadísticos no identificables individualmente; 4. Se prohíbe el acceso a datos personales de terceros, salvo en casos excepcionales previstos por la ley. 5. Se prohíbe la atribución a los ciudadanos de un número nacional único; 6. Se garantiza a todos el libre acceso a las redes informáticas de uso público, determinando la ley el régimen aplicable a los flujos de datos transfronterizos y las formas adecuadas de protección de datos personales y de otros cuya salvaguardia se justifique por razones de interés nacional; y 7. Los datos personales que consten en ficheros manuales gozan de protección idéntica a la prevista en los apartados anteriores, en los términos que establezca la ley.

partidos o sindicatos, confesión religiosa, vida privada y origen étnico, salvo con el consentimiento expreso del titular, lo que proporciona garantías de no discriminación. Igualmente, se garantiza a todos el libre acceso a las redes informáticas de uso público, determinando la ley al régimen aplicable a los flujos de datos transfronterizos y las formas adecuadas de protección de datos personales y de otros, cuya salvaguardia se justifique por razones de interés nacional.

B. Ley de la materia

Ley de Protección de Datos Personales No. 67/98 es la norma que actualmente regula la protección de datos en Portugal, sin embargo desde su previsión constitucional hasta que se desarrolló esta disposición hubo de pasar más de una década.

La Constitución portuguesa consagra en 1976 el derecho de protección de datos personales como derecho fundamental, y no es sino hasta pasados 15 años, que surge la primera ley de protección de datos, la *Ley 10/91*, de 29 de Abril de 1991, la cual regula la utilización y control de los datos personales, y en la que se prevé la creación de la Comisión Nacional de Protección de Datos Personales Informatizados (CNPDPI). Así, estando ya en funciones la Comisión, la referida ley sufre algunas alteraciones con la *Ley 28/94*, de 29 de Agosto, que aprueba medidas que refuerzan la protección de datos personales.

En el año 1995 es publicada la Directiva Europea 95/45/CE de protección de datos personales, misma que condujo a la realización de la conducente reforma constitucional en 1997. En 1998 es aprobada la nueva ley de protección de datos personales: la *Ley 67/98*, de 26 de Octubre, que transpone dicha Directiva en la normatividad portuguesa. Esta viene a alargar substancialmente la serie de atribuciones y competencias de la Comisión, que pasa desde entonces, de CNPDPI a llamarse Comisión Nacional de Protección de Datos.

C. Autoridad garante

La Comisión Nacional de Protección de Datos, es la institución encargada de velar por el debido cumplimiento del derecho de PDP, inició su primer

mandato el 7 de enero de 1994, comenzando físicamente en su actual sede frente a la Asamblea de la República.

En 1997, se hacen algunos cambios al artículo 35 constitucional de modo que permita una adecuada transposición de la Directiva 95/46/CE, en cuya redacción consagra la existencia constitucional de la Comisión como una entidad administrativa independiente. Así en 1998 se aprueba la nueva ley de protección de datos que actualmente se encuentra en vigor en Portugal.

9.2 Alemania

A. Constitución

La Ley Fundamental para la República Federal de Alemania, es la Constitución de 23 de Mayo de 1949⁹⁶, publicada en Bonn y contiene únicamente disposiciones que regulan el derecho a la privacidad. Los artículos que garantizan el derecho a la vida privada y a la dignidad humana, son los siguientes:

El art. 1 refiere la protección de la dignidad humana y la vinculación del poder estatal a los derechos fundamentales. En él se establece que la dignidad humana es intangible, siendo obligación de todo poder pública respetarla y protegerla. Reconoce además la inviolabilidad e inalienabilidad de los derechos

⁹⁶ El Consejo Parlamentario comprobó en sesión pública el 23 de mayo de 1949 en Bonn, que la Ley Fundamental para la República Federal de Alemania, acordada el 8 de mayo de 1949 por el Consejo Parlamentario, fue aprobada en la semana del día 16 al 22 de mayo de 1949 por las representaciones del pueblo de más de los dos tercios de los Länder alemanes participantes. En virtud de esta comprobación, el Consejo Parlamentario, representado por su Presidente, sancionó y promulgó la Ley Fundamental. Así pues, y conforme al art. 145, inciso 3, se publica la Ley Fundamental en el Boletín Oficial Federal. Esta orden de publicación apareció en la primera edición del Boletín Oficial Federal, con fecha 23 de mayo de 1949.

humanos⁹⁷. Por su parte el art. 10 de la Constitución alemana, consagra el la inviolabilidad del secreto epistolar, postal y de telecomunicaciones⁹⁸.

El art. 13 constitucional consagra la inviolabilidad del domicilio, estableciendo que los registros no podrán ser ordenados sino por el juez y, si la demora implicare un peligro inminente, también por los demás órganos previstos por las leyes, y únicamente en la forma estipulada en ellas.

B. Ley de la materia

La Ley Federal de Protección de Datos (*Federal Data Protection Act*) del 15 de Noviembre de 2006, es la normatividad vigente en Alemania, que existe desde 1977. Es la ley principal que se encarga de desarrollar la legislación facultada para proteger los datos personales, dado que este derecho, no se encuentra regulado como tal dentro de la Constitución alemana.

Emilio Suñé Llinás (2002: 57-58) refiere características interesantes de esta Ley como que facilita muchísimo la ósmosis de datos entre las distintas dependencias públicas, cuestión que le parece discutible puesto que la comunicación entre ellas puede ser en perjuicio del ciudadano. Asimismo cabe la comunicación pública de datos al sector privado si se acredita un interés legítimo y no se perjudican intereses dignos de protección al afectado. Además permite comercializar con datos personales automatizados, siempre que se tomen de fuentes de general acceso y sin necesidad de informar al afectado. También, nos dice que lo más original de la ley alemana es la necesaria creación en al empresa

⁹⁷ Artículo 1, sobre la protección de la dignidad humana, vinculación de los poderes públicos a los derechos fundamentales: 1. La dignidad humana es intangible. Respetarla y protegerla es obligación de todo poder público; 2. El pueblo alemán, por ello, reconoce los derechos humanos inviolables e inalienables como fundamento de toda comunidad humana, de la paz y de la justicia en el mundo; y 3. Los siguientes derechos fundamentales vinculan a los poderes legislativo, ejecutivo y judicial como derecho directamente aplicable. Por su parte, el artículo 2, sobre la libertad de acción y de la persona: 1. Toda persona tiene el derecho al libre desarrollo de su personalidad siempre que no viole los derechos de otros ni atente contra el orden constitucional o la ley moral; y 2. Toda persona tiene el derecho a la vida y a la integridad física. La libertad de la persona es inviolable. Estos derechos sólo podrán ser restringidos en virtud de una ley.

⁹⁸ Artículo 10. Secreto epistolar, postal y de telecomunicaciones. 1. El secreto epistolar, así como el secreto postal y de las telecomunicaciones son inviolables; y 2. Las restricciones sólo podrán ser ordenadas en virtud de una ley. Si la restricción está destinada a proteger el régimen fundamental de libertad y democracia o la existencia o seguridad de la Federación o de un *Land*, la ley podrá disponer que no se informe al afectado y que el recurso jurisdiccional sea remplazado por el control de órganos y de órganos auxiliares designados por los representantes del pueblo.

de un Comisario de Protección de Datos, si dicha empresa elabora datos personales y ocupa en ello permanentemente a más de cinco trabajadores; donde el Comisario depende directamente del gerente u órgano asimilado, pero no está sujeto a sus instrucciones en la materia.

C. Autoridad garante

El Comisario Federal para la Protección de Datos y Libertad de Información (*Federal Commissioner for Data Protection and Freedom of Information*), es la institución especializada en la materia, el cual depende directamente del Ministerio del Interior.

D. Sentencia de 15 de Diciembre de 1983, contra la Ley del Censo

Esta sentencia es el resultado de un Recurso de Amparo constitucional (Reclamación constitucional) presentado el 5 de marzo de 1983, en contra de la Ley del Censo de Población del mismo año, aprobada por el *Bundestag* el 4 de marzo de 1982 y publicada el 31 de marzo⁹⁹. El recurso invocaba que la ley lesionaba derechos protegidos por la Ley Fundamental de Bonn, los cuales eran: a) el derecho al libre desenvolvimiento de la personalidad y a la dignidad humana; b) la libertad de expresión y; c) las garantías procesales.

Los recurrentes alegaban en esencia la violación de sus derechos, mediante el formulario que la persona debía contestar, ya que a través del mismo se obtenía información muy precisa y detallada del ciudadano, y todos los datos relacionados con la persona en lo particular, so pena de sanciones pecuniarias. Asimismo, alegaban la necesidad de la garantía del anonimato exigida para las investigaciones con fines estadísticos; ya que sin dicho respaldo, toda encuesta es susceptible de ser utilizada con fines ajenos a los perseguidos, y de que la persona se vea vulnerada en su derecho a la autodeterminación informativa.

Según los demandantes, las oficinas regionales de estadística se habían convertido en centrales regionales de datos, y numerosas administraciones

⁹⁹ Tribunal Constitucional Alemán, sentencia de 15 de diciembre de 1983, publicada en BJC Boletín de Jurisprudencia Constitucional, número 33, enero 1984, Publicaciones de las Cortes Generales, Madrid. Trad. Manuel Daranas. pp. 126-170.

especiales habían introducido sus propios bancos de información con distintivos personales propios, y que a escala municipal el padrón se había ido convirtiendo cada vez más en un banco omnicomprendivo de datos sobre los habitantes, datos que eran en principio reclamables por cualquier oficina estatal. Todo ello, a consecuencia de que la información era manejada por las mismas computadoras y personas. De ahí que las garantías tradicionales para la protección eficaz de los datos ya no eran suficientes.

Por esta evolución de las condiciones tecnológicas, ya era posible producir una imagen total y pormenorizada de la persona –un perfil de la personalidad-, incluso en el ámbito de su intimidad, convirtiendo así al ciudadano, en el llamado “hombre de cristal”.

Para resolver este caso el Tribunal Constitucional alemán parte de la garantía establecida en la Constitución alemana por el art. 2.1, conocida como el “derecho general de la personalidad”. Este garantiza un ámbito de autonomía, de desarrollo de la vida privada, en el que el sujeto puede desarrollar su propia individualidad. Este derecho protege la representación o imagen que el individuo quiere hacer de sí mismo en la sociedad, del que se pueden desprender otros derechos, como el de la propia imagen, la palabra, el honor, la resocialización, la sexualidad, la familia, el matrimonio, la autodeterminación informativa y finalmente, protege contra cualquier otra injerencia que se produzca en relación con la esfera privada (Arenas Ramiro, 2006: 387-388 y Pérez Luño, 1999: 317).

Por el momento el tema que más nos interesa, es el derecho general de la personalidad protegido por el art. 2, párr. 1, en relación con el art. 1, párr. 1 de la Ley Fundamental. Esto es, el valor y la dignidad de la persona, que actúa con libre autodeterminación como miembro de una sociedad libre. En cuanto a la importancia de la dignidad, Pérez Luño (1999: 49) dice que ésta ha sido en la historia, y es en la actualidad el punto de referencia de todas las facultades que se dirigen al reconocimiento y afirmación de la dimensión moral de la persona; y que por lo tanto su jerarquía en la génesis de la teoría moderna de los derechos humanos es innegable.

El Tribunal Constitucional alemán, estima que esa autodeterminación individual, presupone que se le conceda al individuo la capacidad de decisión sobre las acciones, tanto a realizarlas, como a omitirlas. Esto además supone al individuo la capacidad de saber y disponer qué información de si mismo sea la que circule y se encuentre en posesión de determinados sectores de la sociedad o autoridad. Por lo que no sería compatible con el derecho a la autodeterminación informativa, un orden social y jurídico en el que el individuo se sienta inseguro ante la imposibilidad de controlar sus datos personales, es decir, cuando el ciudadano ya no es capaz de saber quién, qué, cuándo y con qué motivo sabe algo de él.

El Tribunal precisa que el derecho a la “autodeterminación informativa” no está garantizado sin límites, y que el individuo no tiene derecho sobre sus datos con soberanía absoluta. Toda vez que dicha información también es un reflejo de la realidad social, y por tanto, en este sentido también habrá de tener límites para la consecución de los fines del Estado, que incluyen los intereses de la sociedad¹⁰⁰.

¹⁰⁰ Las leyes sobre cotejo de matrículas de los *Länder Hessen* y *Schleswig-Holstein* de investigación online (BVerfG, 1 BvR 2074/05 vom 11.3.2008) del *Land Nordrhein-Westfalen* le brindan al Tribunal Constitucional Federal alemán, la ocasión perfecta para abordar los límites que el derecho a la autodeterminación informativa impone a la política antiterrorista. Por lo que respecta al cotejo de matrículas (BVerfG, 1 BvR 370/07 vom 27.2.2008), las leyes de *Hessen* y *Schleswig-Holstein* preveían que, en el marco de la lucha antiterrorista, se almacenaran números de matrículas arbitrariamente seleccionadas. Con este fin los coches eran grabados mediante una videocámara, se extraía el número de matrícula y se volcaba en los ficheros de la policía. Si se conseguía alguna coincidencia, la policía recibía un aviso, si no la había, los datos eran cancelados y desaparecían de los archivos. Como el derecho más afectado por esta medida era la protección de datos personales, el Tribunal Constitucional Federal comienza la sentencia reiterando su conocida jurisprudencia sobre el derecho a la “autodeterminación informativa”. Por ello, le recuerda al legislador que el ciudadano, para ser libre, necesita determinar o, al menos, saber qué información concerniente a su persona está disponible en las distintas esferas. Dado que no existen datos inocuos *per se*, el tratamiento de números de matrícula puede lesionar le derecho. No habría amenaza al derecho si fueran anónimos durante todo el proceso y, además, se destruyesen una vez se contrastasen las matrículas con los ficheros policiales. Pero en el momento en que se produce la coincidencia entre el fichero y el número de matrícula, comienza un peligro concreto para la libertad de acción y la privacidad de la persona, el derecho a la autodeterminación informativa protege. Si el poder público sabe a qué hora pasa un coche y por dónde, puede conocer también otras actividades del dueño del coche y de sus acompañantes. Si un aparato de video vigilancia está cerca de un lugar en el que se celebra una reunión, permite suponer la participación del ciudadano, pudiendo interferir en el ejercicio del derecho de reunión (González Pascual, 2009: 947-948).

9.3 Francia

A. Constitución

La Constitución francesa de 1958 (V República) no contiene un apartado de derechos fundamentales del individuo, ésta se concreta solo a regular la estructura y organización gubernamental del Estado. La garantía de los derechos humanos actuales se ve protegida por el preámbulo de la Constitución, al referir que el pueblo francés proclama solemnemente su adhesión a los derechos humanos y a los principios de la soberanía nacional tal y como fueron definidos por la Declaración de 1789, confirmada y completada por el Preámbulo de la Constitución de 1946.

La Declaración de Derechos del Hombre y del Ciudadano de 1789¹⁰¹, por datar del siglo XVI, actualmente carece de la gran parte de los derechos fundamentales concebidos para la sociedad de hoy en día, por ello, la lista de derechos se ve corregida en 1946. Esta ampliación de derechos, al catálogo, omite el derecho a la privacidad o a la protección de datos personales, pese a ser Francia uno de los países pioneros en la materia.

Es así que, ni la Constitución, ni la Declaración, o el preámbulo constitucional de 1946, contienen mención alguna del derecho a la autodeterminación informativa. No obstante ello, los derechos fundamentales de los ciudadanos se encuentran protegidos por la adhesión de Francia a los tratados y convenios internacionales, como es el caso de los contenidos en la Declaración Universal de Derechos Humanos y de los convenios europeos en materia de derechos humanos.

B. Antecedente histórico

En 1970 el Instituto Nacional de Estadística emprendió un proyecto de monitoreo ciudadano, denominado SAFARI (*Système Automatisé pour les Fichiers Administratifs et le Répertoire des Individus*). Lo que pretendía, era la

¹⁰¹ La Declaración es aprobada el 26 de Agosto de 1789, y se produce en el seno de un ambiente revolucionario que supone el paso del Estado absoluto al Estado liberal, de una sociedad estamental o castas a una de clases, y de una economía feudal a una economía capitalista (Martínez de Pisón, 1997: 75).

asignación de un número único a cada persona, para ser identificada en cada una de sus relaciones con la administración pública. Sin embargo, la reacción de fuerte protesta general y la controversia popular que se generó a raíz de la pretensión de implantar dicho proyecto, hicieron que finalmente se optara, por parte del gobierno francés en 1974, por la creación de una comisión especializada (García-Berrio, 2003: 165); ésta sería responsable de estudiar el avance tecnológico y la protección del respeto de las libertades personales.

C. Ley de la materia

La ley relativa a la informática, los ficheros y las libertades (*loi relative à l'informatique, aux fichiers et aux libertés*) es producto de la polémica originada en torno al proyecto SAFARI, y nace el 6 de enero de 1978 la Ley “Informática y Libertades”. Se compone de 72 artículos, divididos en 13 títulos, y es hoy en día un instrumento que parece ser muy moderno comparado con los demás Estados miembros de la Unión Europea. La Directiva 95/46/CE, de 24 de octubre de 1995, se inspira en gran medida en ésta ley. Por ello, Francia no se ve en la necesidad de transponer inmediatamente dicha Directiva dentro del ordenamiento interno. La reforma de 2004 modifica profundamente dicho ordenamiento, y es así que actualmente, la ley francesa, en materia de protección de datos personales sigue estando un paso adelante¹⁰².

Entre las innovaciones de esta ley, destacan su manera de enfocar la protección de los datos personales y de poner en práctica sus principios, la idea de responsabilidad de las empresas en la aplicación de la ley (reconocimiento del interés de la autorregulación), pero también la de los ciudadanos en la protección de sus derechos. Así mismo, se han tenido en cuenta todas las posibilidades de simplificación y exoneración de la notificación, incluso en caso de designación de un “encargado de protección de los datos personales”. La mayor innovación es un

¹⁰² Para mayor abundamiento se puede consultar el documento titulado “la ley francesa de protección de datos de carácter personal”, proporcionado por Alex Türk, Presidente desde 2004, de la Comisión Nacional de Informática y Libertades (CNIL), en Francia. Dicho documento, fue presentado dentro de las jornadas del curso de verano: Hacia un nuevo Reglamento de la Ley Orgánica de Protección de Datos; llevadas a cabo del 27 de junio al 1º de julio de 2005, en Santander, España. El documento está disponible en: http://www.cnil.fr/fileadmin/documents/es/La_ley_francesa_de_proteccion_de_datos.pdf (consulta: 09/11/2012).

reequilibrio entre el *control previo* de la creación de los tratamientos (que siempre ha sido el modo de acción privilegiado de la Comisión Nacional de Informática y Libertades), y el *control a posteriori*, especialmente a través de la instrucción de las quejas, las inspecciones y algo totalmente nuevo, el ejercicio de la potestad sancionadora¹⁰³.

D. Autoridad garante

La Comisión Nacional de Informática y Libertades (*Comission Nationale de l'Informatique et des Libertés*) es el órgano oficial de aplicar la ley francesa de protección de datos de carácter personal de 1978 (reformada en el 2004), y creada por esta misma ley. Se trata de un órgano único con competencia nacional que consiguió en su creación ser la primera de las llamadas autoridades administrativas independientes, una nueva categoría de ente de derecho público. Es una institución del Estado, pero que no está sometida a la autoridad jerárquica de ningún ministro.

Es un órgano colegial que se compone de 17 comisarios: 2 diputados, 2 senadores, 2 miembros del Consejo de Economía y Social, 6 representantes de alta jurisdicción (2 Consejeros de Estado, 2 de la Corte de Casación y 2 de la Corte de Cuentas), y 5 personas calificadas (1 por el Presidente de la Asamblea Nacional, 1 por el Presidente del Senado y 3 por el Consejo de ministros).

9.4 España

A. La Constitución

La Constitución de España de 27 de Diciembre de 1978¹⁰⁴, garantiza el derecho a la intimidad y la propia imagen (art. 18 CE). Específicamente, el art. 18.4 CE protege el derecho a la intimidad limitando el uso de la informática, idea que se encuentra intrínsecamente ligada a la protección de datos personales, que se concibe hoy en día a partir de la era informática.

¹⁰³ Al respecto véase a Suñé Llinás (2002: 59-60).

¹⁰⁴ La Constitución de España fue aprobada por las Cortes en sesiones plenarias del Congreso de los Diputados y del Senado celebradas el 31 de octubre de 1978, ratificada por el Pueblo Español en referéndum de 6 de diciembre de 1978, y sancionada por S.M. el Rey ante las Cortes el 27 de diciembre de 1978.

El título del artículo 18 constitucional, sin embargo, es sobre el derecho a la intimidad e inviolabilidad del domicilio. En el mismo, se garantiza el derecho al honor, a la intimidad personal y familiar y a la propia imagen. Asimismo, refiere la inviolabilidad del domicilio y el secreto de las comunicaciones. Además, de limitar el uso de la informática para gestionar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos¹⁰⁵.

B. Ley de la materia

La Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (BOE 14/12/1999), establece que tendrá por objeto garantizar y proteger, en lo concerniente 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.

Esta LOPD viene a sustituir a la Ley Orgánica 5/1992, de 29 de octubre, de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal (LORTAD), la cual estuvo vigente hasta el 14 de enero del 2000.

C. Autoridad garante

El art. 35 LOPD establece que la Agencia de Protección de Datos 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. Entre éstas, se encuentra la de velar por el cumplimiento de la legislación sobre protección de datos y controlar su aplicación, en especial en lo relativo a los derechos de información, acceso, rectificación, oposición y cancelación de datos. Así mismo deberá de proporcionar información a las personas acerca de sus derechos en materia de tratamiento de sus datos personales (art. 37 LOPD).

¹⁰⁵ Artículo 18. 1. Se garantiza el derecho al honor, a la intimidad personal y familiar y a la propia imagen; 2. El domicilio es inviolable. Ninguna entrada o registro podrá hacerse en él sin consentimiento del titular o resolución judicial, salvo en caso de flagrante delito; 3. Se garantiza el secreto de las comunicaciones y, en especial, de las postales, telegráficas y telefónicas, salvo resolución judicial; y 4. 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.

III. PROTECCION DE DATOS PERSONALES EN ESPAÑA

Internet ha crecido de una forma inimaginable, en la que hoy en día se vive un bombardeo de información, asimismo hay una gran cantidad de transmisión de datos producto de nuestro paso y actividad por los diferentes sitios de la red. Lucas Murillo de la Cueva (2000: 89) dice que el problema del ritmo desigual de desarrollo de la tecnología informática, es que atenta a conseguir cada día nuevas metas, y no se ha preocupado al mismo tiempo, de la seguridad de la información; y que mientras se preocupó de abrir nuevas fronteras, descuidó la protección eficiente de los instrumentos que ha ido creando.

Martínez Martínez (2004: 50) refiere que la informática y su confluencia con las telecomunicaciones comporta un salto cualitativo en la dimensión informacional de la privacidad, ya que por una parte es posible obtener información sobre comportamientos individuales mediante el tratamiento de información que aisladamente considerada no revelaría aspectos privados. Por otro lado, el software, se diseña de modo que es capaz de rastrear y almacenar las pautas de comportamiento de los usuarios en Internet sean estos o no conscientes. Y que por último, en el contexto de la llamada nueva economía, el flujo de información personal adquiere un valor determinante y, por primera vez en la historia, una dimensión global.

En España aparece el derecho a la protección de datos personales de forma paulatina. En el art. 18.4 CE se comienzan a percibir los indicios de este, al referir que la ley limitará el uso de la informática, para garantizar el honor y la vida privada y familiar. En este apartado también se precisaran las distintas Sentencias del Tribunal Constitucional español, que han configurado histórica y jurisprudencialmente el derecho a la protección de datos personales.

1. La Constitución de España y el contenido del artículo 18

El art. 10 CE¹⁰⁶, establece el fundamento del orden político y de la paz social del país, sentado en la base de la dignidad de la persona y el desarrollo de

¹⁰⁶ Art. 10 CE. Derechos de la persona. “1. 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

la personalidad, entre otros. Estos, son los principios en los cuales descansa el derecho a la protección de datos personales (como derecho autónomo) y son también las objetivos principales que busca la protección de la vida privada, la cual se puede proteger ejerciendo el derecho a la protección de datos personales¹⁰⁷.

El art. 18 CE protege el derecho a la intimidad e inviolabilidad del domicilio. Los derechos consagrados en este dispositivo, aparecen como derechos fundamentales estrictamente vinculados a la propia personalidad, derivados sin duda de la “dignidad humana”, que reconoce el artículo 10 CE y que implican la existencia de un ámbito propio y reservado frente a la acción y conocimiento de los demás, necesario –según las pautas de la cultura española- para mantener una calidad mínima de la vida humana¹⁰⁸. El art. 18 CE se sitúa en la Sección I del Capítulo II del Título I, titulado “De los Derechos Fundamentales y las Libertades Públicas”, de ahí su importancia, nivel de protección y posibilidad de solicitar recurso de amparo. Así el art. 18.4 CE, establece que la ley limitará el uso de la informática en favor del honor, la intimidad personal y familiar.

Respecto a los derechos contemplados en el art. 18 CE, se pone de manifiesto que en tanto el art. 8.1 CEDH reconoce el derecho de toda persona “al respeto de su vida privada y familiar, de su domicilio y de su correspondencia”, el

los demás son fundamento del orden político y de la paz social. 2. Las normas relativas a los derechos fundamentales y a las libertades que la Constitución reconoce se interpretarán de conformidad con la Declaración Universal de Derechos Humanos y los tratados y acuerdos internacionales sobre las mismas materias ratificados por España”. Llama la atención, la diferencia de cómo es referida la DUDH en las Constituciones española y mexicana, en lo que hace a la enumeración de los derechos fundamentales y libertades de la persona. La primera remite, casi desde el principio del texto, directamente a dicha Declaración, así como a los tratados y acuerdos internacionales ratificados por España; mientras que en la mexicana, no es sino hasta el art. 133, que reconoce los derechos establecidos en los tratados internacionales celebrados por el país (que a la letra dice: Esta Constitución, las leyes del Congreso de la Unión que emanen de ella y todos los Tratados que estén de acuerdo con la misma, celebrados y que se celebren por el Presidente de la República, con aprobación del Senado, serán la Ley Suprema de toda la Unión. Los jueces de cada Estado se arreglarán a dicha Constitución, leyes y tratados, a pesar de las disposiciones en contrario que pueda haber en las Constituciones o leyes de los Estados.

¹⁰⁷ Así lo estableció la Sentencia del Tribunal Constitucional Federal alemán sobre la Ley del Censo de Población de 15 de diciembre de 1983. En ésta, el Tribunal entendió que el individuo podía ver limitado su desarrollo personal y ver afectada su dignidad sino actuaba con total libertad, y que no actuaría con total libertad si no sabía qué datos sobre él se estaban manejando o eran conocidos (Arenas Ramiro, 2006: 397).

¹⁰⁸ La STC 231/1988, FJ 3, refiere además que esos derechos -imagen, intimidad personal y familiar, y dignidad humana- se muestran como personalísimos y ligados a la misma existencia del individuo (Así también queda asentado en la STC 214/1991, FJ 1).

art. 18 CE precisa diferenciadamente los derechos fundamentales a la intimidad personal y familiar (art. 18.1 CE) y a la inviolabilidad del domicilio (art. 18.2 CE). En el primero, se ha advertido que su objeto hace referencia a un ámbito de la vida de las personas excluido tanto del conocimiento ajeno como de las intromisiones de terceros, y que la delimitación de este ámbito ha de hacerse en función del libre desarrollo de la personalidad. De acuerdo con este criterio, uno de dichos ámbitos de exclusión, es el domiciliario por ser aquel en el que los individuos, libres de toda sujeción a los usos y convenciones sociales, ejercen su libertad más íntima (STC 119/2001, FJ 6).

1.1 Derecho al honor, a la intimidad personal y familiar y a la propia imagen

Los derechos al honor, intimidad personal y familiar y a la propia imagen, contemplados en el art. 18 CE, son derechos autónomos. En su condición de derechos de la personalidad, derivados de la dignidad y dirigidos a proteger el patrimonio moral de las personas, guardan entre sí una estrecha relación (STC 81/2001¹⁰⁹, FJ 2). De este modo, al tener cada uno de ellos su propia sustantividad, la apreciación de la vulneración de uno no conlleva necesariamente la vulneración de los demás (STC 156/2001¹¹⁰, FJ 2).

A) Derecho al honor

El honor, es un derecho de la personalidad que suele clasificarse dentro de los de proyección social, especie de patrimonio moral de la persona, condiciones

¹⁰⁹ En la demanda de amparo se argumenta que el recurrente, conocido actor, había popularizado una peculiar forma de vestir en sus apariciones televisivas, que se reproduce en ese anuncio publicitario; y que, además, fue compositor e intérprete de una canción titulada «Me huelen los pies». Estos elementos, incorporados a la publicidad, permitían identificar la imagen del actor, que habría sido explotada comercialmente por la entidad demandada sin su consentimiento. Se sostiene asimismo que, contrariamente a lo declarado en la Sentencia del Tribunal Supremo, en el anuncio controvertido queda plenamente identificada la figura del recurrente sin necesidad de haber reproducido su cara o utilizar su nombre y que al tratarse de la utilización comercial de la imagen, el objeto de protección no es la imagen en su sentido estricto, sino la *identidad personal* puesto que en casos de personajes famosos no es necesario utilizar sus rasgos físicos identificadores para que esa persona pueda ser reconocida (STC 81/2001, FJ 1). A este efecto el Tribunal desestimó el recurso por no suponer, el caso en concreto, una vulneración del derecho constitucional a la propia imagen garantizado por el art. 18.1 CE.

¹¹⁰ La demandante de amparo alega que la Sentencia del Tribunal Supremo vulnera su derecho al honor, pues considera que, en lo que a ella se refiere, la revista no ha demostrado la veracidad del texto publicado. De igual modo sostiene que, al haberse difundido fotografías suyas desnuda y haberle atribuido la autoría de unos manuscritos de carácter estrictamente privado e íntimo, se han vulnerado sus derechos a la intimidad y a la propia imagen (STC 156/2001 de 12 de julio, FJ 1). En este sentido el Tribunal si encontró una vulneración al derecho a la propia imagen.

que ésta considera expresión concreta de su propia estimación, es decir y en un sentido objetivo, como reputación, esto es, la opinión o estima que de la persona tienen los demás (Caballero Gea, 2007: 21). Hablar de honor y su evolución, desde sus inicios, hasta su constitucionalización, es reconocer que ha costado en la cultura jurídica alcanzar el absoluto reconocimiento de este derecho como vinculado a la dignidad e inseparable de la personalidad sin matices. Durante el siglo XIX empieza a hablarse de diferentes tipos de honor, el cual dependería de la clase social u oficio, mismo que se defendía a través de la acción privada como el duelo (Callejo Carrión, 2006: 25-26).

El derecho al honor es un derecho de la personalidad, y como tal, está directamente relacionado con la dignidad de la persona. En la doctrina se ha aceptado la definición acuñada por la italiana, la cual lo define como la dignidad personal reflejada en la consideración de las demás y en el sentimiento de la propia persona (Granados Pérez, 1999: 137-138)¹¹¹.

El honor constituye un concepto jurídico indeterminado cuya delimitación depende de las normas, valores e ideas sociales vigentes en cada momento y que presenta una variedad de concepciones a través de la historia. Por ello, que los órganos judiciales dispongan de un cierto margen de apreciación a la hora de concretar en cada caso qué acto será lesivo del derecho al honor. A pesar de ello, el Tribunal Constitucional español no ha renunciado a intentar definir el contenido constitucional abstracto dicho derecho fundamental, y ha afirmado que, este ampara la buena reputación de una persona, protegiéndola frente a expresiones o mensajes que puedan hacerla desmerecer en la consideración ajena al ir en su descrédito o menosprecio o al ser tenidas en el concepto público por afrentosas (STC 180/1999, FJ 4)¹¹².

Asimismo, el Tribunal ha establecido que el honor es un derecho fundamental protegido por la Constitución, que deriva de la dignidad de la persona. De manera que, salvo que los propios actos lo disminuyan socialmente,

¹¹¹ Granados Pérez (1999: 138), refiere que el derecho al honor ha de tratarse de una persona viva, pues, la persona fallecida no puede ser titular del derecho al honor en cuanto derecho personalísimo que se extingue con la muerte.

¹¹² SSTC STC 216/2006, FJ 7; 180/1999 y 297/2000, FJ 7.

su titular tiene derecho al respeto y reconocimiento de la dignidad personal que se requiere para el libre desarrollo de la personalidad en la convivencia social, sin que pueda ser escarnecido o humillado ante uno mismo o los demás (STC 219/1992, FJ 2). La dignidad como rango o categoría de la persona como tal, del que deriva y en el que se proyecta el derecho al honor, no admite discriminación alguna por razón de nacimiento, raza, opiniones o creencias¹¹³.

Es de precisar que, si bien el concepto de intimidad es objeto de constante estudio por la doctrina, la protección que confiere el derecho a la intimidad, alcanzaría a todas aquellas manifestaciones de la vida de una persona que constituyen su esfera más personal en sus tres facetas: personal, familiar y social. Estas, sirven para cumplir las finalidades de autodefensa, autorrealización personal y conformación de vínculos afectivos, concediendo al sujeto un haz de facultades que le permiten preservar dichas facetas del conocimiento ajeno y controlar la obtención de datos personales, que pertenecen a esta esfera y de aquellos otros que, aunque no estrictamente íntimos, puedan contribuir a la configuración de su perfil psicológico, pese a que tales informaciones, analizadas de forma aislada, pueden carecer de trascendencia.

En la Constitución española, el derecho al honor (en el contexto de asuntos de relevancia pública) tiene un significado personalista, es decir, hace referencia a personas individualmente consideradas. Por lo tanto, hace inadecuado hablar del honor de las instituciones públicas o de clases determinadas del Estado, respecto de las cuales es más correcto, desde el punto de vista constitucional, emplear los términos de dignidad, prestigio y autoridad moral, que son valores que merecen la protección penal que les dispense el legislador, pero que no son exactamente identificables con el honor, consagrado en la Constitución como derecho fundamental, y, por ello, en su ponderación frente a la libertad de expresión debe asignárseles un nivel más débil de

¹¹³ El odio y el desprecio a todo un pueblo o a una etnia (a cualquier pueblo o a cualquier etnia) son incompatibles con el respeto a la dignidad humana, que sólo se cumple si se atribuye por igual a todo hombre, a toda etnia, a todos los pueblos (STC 214/1991, FJ 8).

protección del que corresponde atribuir al derecho al honor de las personas públicas o de relevancia pública (STC 107/1988¹¹⁴ de 8 de junio, FJ 2).

B) Derecho a la intimidad personal y familiar

Con relación al derecho a la intimidad personal y familiar, el Tribunal refiere que este se extiende, no sólo a aspectos de la vida propia y personal, sino también a determinados aspectos de la vida de otras personas con las que se guarde una especial y estrecha vinculación, como es la familiar. Aspectos que, por la relación o vínculo existente con estas personas, inciden en la propia esfera de la personalidad del individuo que protegen los derechos del art. 18 CE. Es de señalar que, sin duda será necesario, en cada caso, examinar de qué acontecimientos se trata, y cuál es el vínculo que une a las personas en cuestión; pero al menos, no cabe dudar que ciertos eventos que puedan ocurrir a padres, cónyuges o hijos tienen, normalmente, y dentro de las pautas culturales de nuestra sociedad, tal trascendencia para el individuo, que su indebida publicidad o difusión incide directamente en la propia esfera de su personalidad. Por lo que existe al respecto un derecho –propio, y no ajeno- a la intimidad, constitucionalmente protegible (STC 231/1988, FJ 4).

El derecho a la intimidad personal y familiar reconocido en el art. 18 CE, al igual que otros, como el derecho a la propia imagen y el honor, aparecen como derechos fundamentales estrictamente vinculados a la propia personalidad, derivados sin duda de la “dignidad de la persona”, reconocida por el art. 10 CE y que implican la existencia de un ámbito propio y reservado frente a la acción y conocimiento de los demás, necesario para mantener una calidad mínima de la

¹¹⁴ Los antecedentes de esta resolución se dan cuando la Sentencia de la Audiencia Provincial dispuso la condena del recurrente como autor de un delito de injurias graves. En esta Sentencia, se detalla que de acuerdo con los hechos probados, un periódico informó, sin firma, que el objetor de conciencia José Navazo, condenado por la Audiencia Provincial por injurias al Ejército, había declarado que «tenía intención de agotar todas las vías jurídicas hasta lograr la absolución». Asimismo, dice la resolución, el procesado habría justificado sus declaraciones explicando que «pretendía definir el papel de los ejércitos a lo largo de la historia; y que no se refería a ningún ejército en concreto» y aseguraba no haber obrado con ánimo de injuriar. El texto con las declaraciones del recurrente en amparo terminaba con las siguientes expresiones: «es increíble que a mí me metan siete meses y que castiguen con un mes de arresto a un capitán de ilustre apellido que llamó cerdo al Rey. Esto me confirma una idea que yo tenía arraigada: hay una gran parte de los Jueces que son realmente incorruptibles; nada, absolutamente nada, puede obligarles a hacer justicia».

vida humana. Se muestran así, esos derechos como personalísimos y ligados a la misma existencia del individuo. Ciertamente, el ordenamiento jurídico español reconoce en algunas ocasiones, diversas dimensiones o manifestaciones de estos derechos que, desvinculándose ya de la persona del afectado, pueden ejercerse por terceras personas¹¹⁵.

La STC 231/1988 de 2 de diciembre de 1988¹¹⁶, es paradigmática y muy ilustrativa en este tema, ya que además de reclamar el derecho a la propia imagen –acción que no prosperó en la vía de amparo–, la demanda de amparo presentó una segunda perspectiva: se invocaron derechos (a la intimidad personal y familiar) cuyo titular no era ya exclusivamente el fallecido, sino, genéricamente, su familia “afectada en su dolor e intimidad”, y, más específicamente su viuda –la demandante–. Desde esta segunda perspectiva, la demanda se centró en el carácter privado que tenía el lugar en que se recogieron determinadas escenas mediante una cámara de vídeo –la enfermería de la plaza de toros– y el carácter íntimo de los momentos en que una persona se debatía entre la vida y la muerte, espacio que debía ser respetado por los demás¹¹⁷. Al tenor de lo anterior el Tribunal sostuvo que esa intimidad no sólo era propia del directamente afectado, sino que, por su repercusión moral, era también un derecho de sus familiares (FJ 4). Lo que interesa de esta resolución es la captación de la imagen en espectáculo público, y la exclusión que hace, como lugar de tal carácter, de la enfermería,

¹¹⁵ STC 231/1988, FJ 3.

¹¹⁶ Esta sentencia es muy particular y famosa, no solo por su trascendencia jurídica, sino además, por la popularidad de la figura pública que interpuso el recurso de amparo (Isabel Pantoja), en el que la recurrente demandaba la protección civil del derecho a la intimidad y a la propia imagen, en contra de una Entidad mercantil (Prographic, SA), sociedad que había realizado y posteriormente comercializado, sin autorización alguna, unas cintas de vídeo en las que se mostraban imágenes de la vida privada y profesional de su difunto marido, don Francisco Rivera Pérez, de profesión torero y conocido públicamente como “Paquirri”, y muy especialmente, imágenes de la mortal cogida que sufrió en la plaza de toros Pozoblanco (Córdoba) y de su posterior tratamiento médico en la enfermería de la citada plaza.

¹¹⁷ Se trata de los momentos en que el torero es introducido en la enfermería y examinado por los médicos; en esas imágenes se reproducen, en forma directa y claramente perceptible, las heridas sufridas, la situación y reacción del herido y la manifestación de su estado anímico, que se revela en las imágenes de sus ademanes y rostro, y que muestra ciertamente, la entereza del diestro, pero también el dolor y postración causados por las lesiones recibidas. Se trata, pues, de imágenes de las que, con seguridad puede inferirse, dentro de las pautas de nuestra cultura, que inciden negativamente, causando dolor y angustia en los familiares cercanos del fallecido, no sólo por la situación que reflejan en ese momento, sino también puestas en relación con el hecho de que las heridas y lesiones que allí se muestran causaron, en muy breve plazo, la muerte del torero. No cabe pues dudar de que las imágenes en cuestión, y según lo arriba dicho, inciden en la intimidad personal y familiar de la recurrente, entonces esposa y después viuda del conocido torero (FJ 6).

argumento que sirvió para anular la Sentencia del Tribunal Supremo. Es decir, “salud y vida del torero” son valores que comienzan a partir de abandonar el coso taurino y entrar en enfermería. Publicitar estas escenas, tal y como lo precisa la propia Sentencia, supondría convertir “en instrumento de diversión y entretenimiento algo tan personal como los padecimientos y la misma muerte de un individuo..., en clara contradicción con el principio de dignidad de la persona” (García García, 2003: 367-368).

La STC 233/1999¹¹⁸, recuerda que la transmisión de información tributaria, ciertamente puede incidir en la intimidad de los ciudadanos (SSTC 110/1984, 45/1989, 142/1993; ATC 462/1996), y concretamente se ha dicho que no hay dudas de que, en principio, los datos relativos a la situación económica de una persona entran dentro de la intimidad constitucionalmente protegida.

C) Derecho a la propia imagen

Por lo que se refiere al derecho a la imagen, se puede considerar paradigmática la STS de 11 de abril de 1987 (RA 2703), que define por primera vez la imagen como “la figura, representación, semejanza o apariencia de una cosa; pero, a efectos de la ley calendada, ha de entenderse que equivale a la representación gráfica de la figura humana mediante un procedimiento mecánico de reproducción y que en tal sentido puede incidir en la esfera de un derecho de la personalidad de inestimable valor para el sujeto y el ambiente social en que se desenvuelve, incluso en sus proyección contra desconocidos sujetos”. Es a partir de esta sentencia que la definición de la imagen se concretiza como la idea de

¹¹⁸ En esta Sentencia, se lleva a cabo una transferencia de datos tributarios y dado que el soporte de la comunicación en estos casos será informático (lo cierto es que, el art. 8.2 a) LHL reclama el establecimiento de la intercomunicación técnica precisa para el trasvase de información «a través de los respectivos Centros de Informática»), los recurrentes entienden que resulta aplicable el art. 18.4 CE, en virtud del cual, 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». Tal circunstancia, sin embargo, no permite afirmar que la remisión que el art. 8.2 c) LHL. hace al reglamento para la determinación del modo en que habrán de transmitirse los datos con trascendencia tributaria en poder de las Administraciones vulnere el citado art. 18.4 CE. Por otro lado, aunque lleguemos a la conclusión de que los hechos con trascendencia tributaria que se pongan de manifiesto en el curso de las actuaciones inspectoras inciden en aspectos de la intimidad tutelada en el art. 18.1 CE, de aquí no cabe derivar tampoco que el art. 8.2 c) L.H.L. transgreda el art. 81.1 CE Como hemos señalado en reiteradas ocasiones, este precepto reclama ley orgánica para el desarrollo de los derechos fundamentales, esto es, como decíamos, entre otras muchas, en la STC 140/1986, para «la determinación de su alcance y límites en relación con otros derechos y con su ejercicio por las demás personas» (fundamento jurídico 5.).

representación gráfica. Así pues, se encuentra en esta definición el doble carácter que tiene este derecho, uno positivo que se traduce en la facultad de la persona para disponer de su imagen y, otro negativo que excluye a otra persona del uso de esta imagen.

En lo que se refiere a los límites del derecho a la propia imagen, la Ley Orgánica 1/1982 (arts. 2 en conexión con el 7, apartados 5 y 6, y art. 8.2) estructura en torno a dos ejes: por una parte, la esfera reservada que la propia persona haya salvaguardado para sí y su familia conforme a los usos sociales; y, por otra, la relevancia o el interés público de la persona cuya imagen se reproduce o de los hechos en que ésta participa, como protagonista o como elemento accesorio. Esta última, constituye una excepción al primer eje, que hace correr paralelo el derecho a la propia imagen con la esfera privada que su titular guarda para sí mismo¹¹⁹. Por otro lado, no puede deducirse del art. 18 CE, que el derecho a la propia imagen, en cuanto límite del obrar ajeno, comprenda el derecho incondicionado y sin reservas a permanecer en el anonimato. Pero tampoco este, como expresión de un ámbito de reserva especialmente amplio, es un valor absolutamente irrelevante quedando desprotegido el interés de una persona a salvaguardarlo impidiendo que su imagen se capte y se difunda (STC 99/1994¹²⁰,

¹¹⁹ Con relación al uso de la imagen de una persona de interés público la STC 23/2010, aborda el hecho de que una revista publica en su semanario, con fin humorístico, una foto manipulada de montaje caricaturesco, implantando la cara de un personaje público en un cuerpo semidesnudo. Ante tal situación la jurisdicción ordinaria condenó a la revista al pago de una indemnización por intromisión ilegítima en el derecho a la propia imagen. Posteriormente, en el recurso de amparo ante el Tribunal Constitucional se alega la vulneración del derecho a la libertad de expresión por la condena a la difusión del montaje fotográfico y los comentarios. La Sentencia rechaza en aplicación de la doctrina de la STC 186/2001 que se haya vulnerado el derecho a la libertad de expresión, ya que la intención de la revista al utilizar la imagen de la afectada era la de provocar, con un marcado sesgo sexista, la burla sobre la persona afectada, a partir exclusivamente de su aspecto físico y obteniendo con ello un beneficio económico para la empresa periodística. Difícilmente se aprecia interés público alguno en este uso de la imagen desvinculado de cualquier finalidad legítima de crítica política o social, de modo que la publicación de la fotografía manipulada en nada contribuye a la formación de una opinión pública libre (FJ 4).

¹²⁰ Esta sentencia aborda un caso peculiarmente interesante, en la que un trabajador (cortador de jamón) fue despedido tras negarse a cortar jamón en un evento organizado por la empresa, con motivo de la muestra de un producto (jamón ibérico) a los medios de comunicación y autoridades autonómicas de la Consejería de Agricultura, para la presentación de la denominación de origen jamón de bellota, fabricado por la empresa en la que prestaba sus servicios el trabajador. El trabajador alegaba que no se negaba a trabajar, solo que no deseaba que bajo ningún concepto su imagen fuese captada fotográficamente. Por lo que la empresa procedió a despedirlo alegando desobediencia en las funciones del trabajador. El Tribunal estimó que deben apreciarse, en este caso como en todos los de colisión de derechos fundamentales o bienes constitucionalmente protegidos, los intereses en presencia, mediante una adecuada ponderación de las circunstancias

FJ 5). En este sentido, el derecho a la imagen se encuentra delimitado así por la propia voluntad del titular del derecho que es, en principio, a quien corresponde decidir si permite o no la captación o difusión de su imagen por un tercero (Caballero Gea, 2007: 64).

Los derechos a la intimidad personal y a la propia imagen, garantizados por el art. 18.1 CE, forman parte de los bienes de la personalidad que pertenecen al ámbito de la vida privada. Salvaguardan estos derechos un espacio de intimidad personal y familiar que queda sustraído a intromisiones extrañas. Y en este ámbito de la intimidad, reviste singular importancia la necesaria protección del derecho a la propia imagen frente al creciente desarrollo de los medios y procedimientos de captación, divulgación y difusión de la misma, así como de datos y circunstancias pertenecientes a la intimidad que garantiza este precepto (STC 170/1987, FJ 5).

Para que se produzca la intromisión ilegítima en el derecho a la propia imagen –a diferencia de lo que ocurre con el derecho al honor– no es preciso que se proceda a la divulgación, es suficiente con la obtención de la imagen o bien que se reproduzca la misma o, en último extremo, que se publique (Crevillen Sánchez, 1994: 96). El art. 7.5 LO 1/1982, refiere como intromisión ilegítima la captación, reproducción o publicación por fotografía de la imagen de una persona en lugares o momentos de su vida privada o fuera de ellos. Ahora bien, es importante señalar que las palabras: captación, reproducción o publicación, no son sinónimos. En esta tesitura, no es de inferir que el consentimiento otorgado para la captación fotográfica, englobe en el mismo la autorización para publicar las imágenes captadas (ATC 300/1989, FFJJ 2 y 3).

A consideración de Balaguer Callejón (1992: 24), la imagen, en cuanto que representa la iconografía del ser humano, es colindante con el derecho al honor y se mezcla en un cierto sentido con este, puesto que una lesión del derecho a la imagen representa la lesión de una parte del honor. Para este autor la jurisprudencia viene confundiendo el derecho al honor con el derecho a la

concurrentes. Por lo que es en esta perspectiva donde ha de situarse la valoración del alcance del derecho a la propia imagen como factor legitimador de la negativa del trabajador a obedecer la orden empresarial (STC 99/1994, FJ 5).

imagen, englobando genéricamente en el honor todos los demás derechos comprendidos en la Ley 1/1982, y dando una mayor importancia al derecho al honor que al derecho a la imagen y a la intimidad, a los que en un cierto sentido considera como derechos secundarios respecto del honor o como claras derivaciones de este¹²¹. Sin embargo, hemos de referir que si bien estos derechos puede parecer que se confunden entre sí, pertenecen a círculos concéntricos, en los cuales casi siempre aparecerán dos o más de estos derechos vulnerados conjuntamente. Balaguer refiere que la Ley tampoco aclara si se trata de un solo derecho al honor, a la intimidad personal y familiar y a la propia imagen, o se trata de tres derechos distintos que se relacionan entre sí¹²². La doctrina viene entendiendo esto último: que son tres derechos de la personalidad con un contenido esencial diferente cada uno de ellos, pero con la relación que es posible mantener entre derechos que se encuentran conectados entre sí.

Se puede decir, que se trata de derechos de la personalidad cuya aproximación en el plano personal es evidente, pero que mantienen diferencias importantes. Para Balaguer Callejón (1992: 26), el concepto de honor e intimidad, no se superponen ni coinciden. Simplemente se relacionan, y lo hacen de manera que no siempre la violación de la intimidad supone descrédito o minusvaloración

¹²¹ En contraposición a esta postura he de referir la STC 216/2006, en su FJ 7, que precisa el contenido del honor, como objeto del derecho consagrado en el art. 18.1 CE, y dice que es «un concepto jurídico indeterminado cuya delimitación depende de las normas, valores e ideas sociales vigentes en cada momento, y de ahí que los órganos judiciales dispongan de un cierto margen de apreciación a la hora de concretar en cada caso qué deba tenerse por lesivo del derecho fundamental que lo protege (SSTC 180/1999; 297/2000, FJ 7). A pesar de ello este Tribunal no ha renunciado a definir el contenido constitucional abstracto del derecho fundamental al honor, y ha afirmado que éste ampara la buena reputación de una persona, protegiéndola frente a expresiones o mensajes que puedan hacerla desmerecer en la consideración ajena al ir en su descrédito o menosprecio o al ser tenidas en el concepto público por afrentosas. Por ello las libertades del art. 20.1 a) y d) CE, ni protegen la divulgación de hechos que, defraudando el derecho de todos a recibir información veraz, no son sino simples rumores, invenciones o insinuaciones carentes de fundamento, ni dan cobertura constitucional a expresiones formalmente injuriosas e innecesarias para el mensaje que se desea divulgar, en las que simplemente su emisor exterioriza su personal menosprecio o animosidad respecto del ofendido. Por contra el carácter molesto o hiriente de una opinión o una información, o la crítica evaluación de la conducta personal o profesional de una persona o el juicio sobre su idoneidad profesional, no constituyen de suyo una ilegítima intromisión en su derecho al honor, siempre, claro está, que lo dicho, escrito o divulgado no sean expresiones o mensajes insultantes, insidias infamantes o vejaciones que provoquen objetivamente el descrédito de la persona a quien se refieran» (STC 49/2001, FJ 5). Asimismo, y para analizar la doctrina del Tribunal Constitucional véase las SSTC 81/2001 y 156/2001.

¹²² La 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, es un ordenamiento que por su momento de elaboración se encarga de regular los cauces legales y no precisamente de regular los derechos.

del honor, ni el honor ha de afectar a esferas de la intimidad necesariamente, sino que cabe una relación contraria. A menudo, sin embargo, el descrédito se lleva a cabo mediante una lesión al derecho a la intimidad.

La imagen constituye un derecho autónomo respecto del derecho a la intimidad y al honor, cuya diferenciación con estos estriba fundamentalmente en que la imagen hace referencia a un derecho propio de lo externo del individuo¹²³, en contraposición a la intimidad, que consiste precisamente en el derecho a que no sean desvelados aspectos íntimos de la personalidad. La imagen también difiere del honor, ya que en este pueden tratarse aspectos externos o internos, pero ambos, deben lesionar la dignidad personal. De ello se infiere que es trascendental en la imagen la actitud del sujeto, y el otorgamiento de su consentimiento para la exhibición (Balaguer Callejón, 1992: 26-27).

Es importante precisar, que el derecho a la propia imagen no puede ser objeto de tutela en vía de amparo, una vez fallecido el titular de ese bien de la personalidad, debido a que no existiría ya, un ámbito vital que proteger en cuanto verdadero objeto del derecho fundamental aun cuando pudieran pervivir sus efectos patrimoniales¹²⁴ (STC 231/1988, FJ 3).

Con relación a este tema la STC 156/2001 en su FJ 3, ha sido claro al declarar que los derechos al honor, a la intimidad y a la propia imagen, a pesar de

¹²³ La imagen de una persona no lo es la representación imaginaria de las características externas de un personaje televisivo (STC 81/2001, FJ 3).

¹²⁴ La Sentencia dice que una vez fallecido el titular de esos derechos, y extinguida su personalidad –según determina el art. 32 del Código Civil: “la personalidad civil se extingue por la muerte de las personas”- lógicamente desaparece también el mismo objeto de protección constitucional, que está encaminada a garantizar, un ámbito vital reservado, que con la muerte deviene inexistente. Por consiguiente, si se mantienen acciones de protección civil (encaminadas como en el presente caso, a la obtención de una indemnización) a favor de terceros, distintos del titular de esos derechos de carácter personalísimo, ello ocurre fuera del área de protección de los derechos fundamentales que se encomienda al Tribunal Constitucional mediante el recurso de amparo. Por ello, y en esta vía, el Tribunal no se pudo pronunciar sobre aquellas cuestiones que, por el fallecimiento del afectado, carecen ya de dimensión constitucional; concretamente, y en el presente caso, sobre la explotación comercial de la imagen del conocido torero en el ejercicio de su actividad profesional. En este aspecto, el “derecho a la imagen” que se invocaba (y al que la demandante concedía especial relevancia) es, en realidad, el derecho a disponer de la imagen de una persona desaparecida y de su eventual explotación económica, protegible, según la LO 1/1982 en vías civiles, y susceptible de poseer un contenido patrimonial, pero derecho que no puede ser objeto de tutela en vía de amparo, ya que, una vez fallecido el titular de ese bien de la personalidad, no existe ya un ámbito vital que proteger en cuanto verdadero objeto del derecho fundamental aun cuando pudieran pervivir sus efectos patrimoniales (STC 231/1988, FJ 3). Sobre la utilización de fotos de víctimas en juicios en Estados Unidos véase a Lyon (2009).

su estrecha relación en tanto que derechos de la personalidad, derivados de la dignidad humana y dirigidos a la protección del patrimonio moral de las personas, tiene, no obstante, un contenido propio y específico. La Sentencia ha dicho que: “mediante la captación y reproducción gráfica de una determinada imagen de una persona se puede vulnerar su derecho a la intimidad sin lesionar el derecho a la propia imagen, lo que sucederá en los casos en los que mediante las mismas se invada la intimidad pero la persona afectada no resulte identificada a través de sus rasgos físicos; en segundo lugar, también puede vulnerarse el derecho a la propia imagen sin conculcar el derecho a la intimidad, supuesto éste que se producirá cuando las imágenes permitan la identificación de la persona fotografiada, pero no entrañen una intromisión en su intimidad; y, finalmente, puede suceder que una imagen lesione al mismo tiempo ambos derechos, lo que ocurriría en los casos en los que revele la intimidad personal y familiar y permita identificar a la persona fotografiada”.

Ahora bien, estos derechos contemplados en el art. 18 CE son los derechos que evolucionan dentro del derecho a la privacidad, para crear, como un derecho único e independiente, el derecho que hoy conocemos como la protección de datos personales, que actualmente encuentra su fundamento en el artículo 18.4 CE, del que hablaremos más adelante.

1.2 Inviolabilidad del domicilio

El domicilio, es concebido como el espacio material donde se desarrolla gran parte de la vida de la persona, y es objeto de protección jurídica desde muy diversos ámbitos. En particular, el Derecho Penal le otorga amparo y esta realidad, por sí sola, evidencia la enorme importancia que se reconoce a dicho espacio, más allá de su simple consideración de refugio privilegiado donde se enmarca una importantísima faceta de la vida: la intimidad (Rodríguez Padrón, 1999: 88). Como se ha dicho antes, el domicilio es el ámbito por excelencia, en el que el individuo es libre de toda sujeción a los usos y convenciones sociales, y es aquí en donde es capaz de ejercer más libremente las distintas facetas de la intimidad (STC 119/2001, FJ 6).

Para Cortés Bechiarelli (1998: 196-197) es ese espacio privado, que sólo pertenece a su titular, el que constituye la base natural para en él desenvolver al máximo la proyección de su yo, de sus intereses, de sus gustos y apetencias, de sus vivencias en suma. Y por lo tanto, es el punto de partida en el desarrollo y desenvolvimiento de la personalidad jurídica en todos los sentidos. Al tenor de ello, nos dice que el derecho a la inviolabilidad del domicilio, constituye –o debería constituir– un freno contra las injerencias, intromisiones o investigaciones arbitrarias de los poderes públicos, especialmente, cuando los miembros de policía pretenden la búsqueda de personas o cosas con propósitos exclusivamente incriminatorios en el lugar o espacio donde se desarrolla la vida privada¹²⁵.

¹²⁵ La STC 22/1984, FJ 5, dice que el art. 18.2 CE contiene dos reglas distintas: una tiene carácter genérico o principal, mientras la otra supone una aplicación concreta de la primera, y su contenido es por ello más reducido. *La primera regla* define la inviolabilidad del domicilio, que constituye un auténtico derecho fundamental de la persona, para garantizar el ámbito de privacidad de ésta, dentro del espacio limitado que la propia persona elige y que tiene que caracterizarse precisamente por quedar exento o inmune a las invasiones o agresiones exteriores, de otras personas o de la autoridad pública. Como se ha dicho acertadamente, el domicilio inviolable es un espacio en el cual el individuo vive sin estar sujeto necesariamente a los usos y convenciones sociales y ejerce su libertad más íntima. Por ello, a través de este derecho no sólo es objeto de protección el espacio físico en sí mismo considerado, sino lo que en él hay de emanación de la persona y de esfera privada de ella. Interpretada en este sentido, la regla de la inviolabilidad del domicilio es de contenido amplio e impone una extensa serie de garantías y de facultades, en las que se comprenden las de vedar toda clase de invasiones incluidas las que puedan realizarse sin penetración directa por medio de aparatos mecánicos, electrónicos u otros análogos. *La segunda regla* establece un doble condicionamiento a la entrada y al registro, que consiste en el consentimiento del titular o en la resolución judicial. La interdicción fundamental de este precepto es la del registro domiciliario, entendido como inquisición o pesquisa, para lo cual la entrada no es más que un trámite de carácter instrumental. Contempladas desde esta perspectiva las cosas, puede extraerse la conclusión de que en toda actividad de ejecución de Sentencias o decisiones llevada a cabo por los órganos públicos, en que se produce, bien que necesariamente, el ingreso de los órganos ejecutores en un domicilio privado, se realiza en mayor o menor medida una inquisición de éste. De la facultad que el titular del derecho sobre el domicilio tiene de impedir la entrada en él es consecuencia que la resolución judicial o la resolución administrativa que ordenan una ejecución que sólo puede llevarse a cabo ingresando en un domicilio privado, por sí solas no conllevan el mandato y la autorización del ingreso, de suerte que cuando éste es negado por el titular debe obtenerse una nueva resolución judicial que autorice la entrada y las actividades que una vez dentro del domicilio pueden ser realizadas. La regla anterior no es aplicable únicamente a los casos en que se trata de una resolución tomada por la Administración en virtud de un principio de autotutela administrativa, como ocurre en el presente caso. A la misma conclusión se puede llegar cuando la decisión que se ejecuta es una resolución de la jurisdicción ordinaria en materia civil. Si los agentes judiciales encargados de llevar, por ejemplo, a cabo un desahucio o un embargo encuentran cerrada la puerta o el acceso de un domicilio, sólo en virtud de una específica resolución judicial pueden entrar. Por consiguiente, el hecho de encontrarse ejecutando una decisión, judicial o administrativa, legalmente adoptada, no permite la entrada y el registro en un domicilio particular. Sin consentimiento del titular o resolución judicial, el acto es ilícito y constituye violación del derecho, salvo el caso de flagrante delito y salvo naturalmente las hipótesis que generan causas de justificación como puede ocurrir con el estado de necesidad.

El art. 18.2 CE, establece que el domicilio es inviolable, por lo que ninguna entrada o registro podrá hacerse en él sin consentimiento del titular o sin resolución judicial, salvo en caso de flagrante delito. Este dispositivo protege la intimidad de la persona, para que nadie pueda vulnerar el derecho al libre desenvolvimiento de la personalidad dentro de su espacio más íntimo, como lo es el hogar, sin previo consentimiento, salvo los casos que expresamente señala la propia Constitución y la jurisprudencia del Tribunal Constitucional¹²⁶. Este último, establece que en el texto constitucional, la norma de interdicción de entrada y de registro sólo admite unas excepciones muy determinadas: el consentimiento del titular, que según el texto del precepto no necesita ser expreso, la existencia de una resolución judicial que la autorice y la producción de un delito flagrante, caso en el cual los perseguidores pueden continuar la persecución del domicilio de la persona afectada (STC 22/1984, FJ 3).

Resulta interesante que la protección a la intimidad dentro del domicilio, es tal, que los sonidos emitidos fuera de este, y que perturben la vida de quienes ahí viven, pueden ser objeto de demanda. En este sentido el Tribunal Constitucional ha dicho que una exposición prolongada a unos determinados niveles de ruido, que pueden objetivamente calificarse como evitables e insoportables, ha de merecer la protección dispensada al derecho fundamental a la intimidad personal y familiar, en el ámbito domiciliario, en la medida en que impidan o dificulten gravemente el libre desarrollo de la personalidad, siempre y cuando la lesión o menoscabo provenga de actos u omisiones de entes públicos a los que sea imputable la lesión producida (STC 119/2001¹²⁷, FJ 6).

¹²⁶ El Juez de Instrucción actúa en estos supuestos como garante del derecho fundamental a la inviolabilidad del domicilio y, en consecuencia, lo único que ha de asegurar es que requiere efectivamente la entrada en él, y la ejecución de un acto que *prima facie*, parece dictado por una autoridad competente en ejercicio de sus funciones, garantizando al mismo tiempo que esa irrupción en el ámbito de la intimidad se produzca sin más limitaciones de ésta (o de otros derechos fundamentales de los ocupantes) que aquellas que sean estrictamente indispensable para ejecutar la resolución administrativa (STC 144/1987, FJ 2).

¹²⁷ En esta sentencia, la recurrente demandaba la indemnización por vulneración de los derechos fundamentales a la vida, salud, intimidad e inviolabilidad del domicilio. La mencionada solicitud, se fundamentaba en una situación de elevada contaminación acústica que vendría padeciendo en su domicilio, consecuencia tanto del efecto auditivo de los ruidos y vibraciones producidos por la multitud de establecimientos molestos ubicados en la zona, declarada por el propio municipio “Zona Acústicamente Saturada”, como por las actividades desarrolladas en una discoteca situada en los bajos de la finca en la que reside, cuyo horario de apertura se prolongaría hasta las 6: 30

1.3 Secreto de las comunicaciones

El artículo 18.3 CE, garantiza el secreto de las comunicaciones y, en especial, de las postales telegráficas y telefónicas¹²⁸, salvo resolución judicial. Así, la carta magna de España, prevé el respeto de la intimidad en las personas mediante la prohibición a todo monitoreo que de su vida se llegará a realizar a través de los medios de comunicación, principalmente –como así lo refiere– las telefónicas y las de correo postal, salvo que medie la correspondiente orden judicial, para que dichos medios de comunicación pudiesen ser intervenidos.

La utilización del correo electrónico es más agresivo para la vida privada que el correo tradicional¹²⁹. En este sentido, el Grupo de trabajo para la protección de datos personales (Grupo de trabajo del art. 29), en su Recomendación núm. 3/97¹³⁰ manifiesta que el correo tradicional es mucho más respetuoso con la intimidad que el electrónico ya que puede enviarse una carta normal sin revelar al propia identidad. El proveedor de servicios postales no puede obtener dato transaccional alguno que permita la identificación del

horas de la mañana. La reclamante reprochaba a la Administración municipal un funcionamiento anormal, al no haber actuado diligentemente en defensa de los derechos e intereses legítimos de los vecinos del lugar, haciendo uso para tal fin de las potestades que le confiere el ordenamiento jurídico. Como resultado de todo ello, la quejosa padecería de insomnio, habiéndose visto obligada a realizar obras de cerramiento de su domicilio para tratar de paliar por sí misma los efectos de la saturación de ruidos.

¹²⁸ La garantía jurisdiccional del secreto de las comunicaciones no se colma con su concurrencia formal -autorización procedente de un órgano jurisdiccional- sino que ésta ha de ser dictada en un proceso, único cauce que permite hacer controlable, y con ello jurídicamente eficaz, la propia actuación judicial. La naturaleza de la intervención telefónica, su finalidad y la misma lógica de la investigación exigen que la autorización y desarrollo de la misma se lleve a cabo, inicialmente, sin conocimiento del interesado, que tampoco participa en su control. Sin embargo, al desarrollarse la actuación judicial en el curso de un proceso, esta ausencia ha de suplirse por el control que en él ejerce el Ministerio Fiscal, garante de la legalidad y de los derechos de los ciudadanos ex art. 124.1 CE, y posteriormente, cuando la medida se alza, el propio interesado ha de tener la posibilidad, constitucionalmente necesaria dentro de ciertos límites que no procede precisar aquí (STEDH caso Klass, núm. 55) de conocer e impugnar la medida. Tal garantía existe también cuando, como en este caso, las de por sí discutibles «diligencias indeterminadas» se unen, pese a todo, sin solución de continuidad, al proceso judicial incoado en averiguación del delito, satisfaciendo así las exigencias de control del cese de la medida que, en otro supuesto, se mantendría en un permanente, y por ello constitucionalmente inaceptable, secreto (STC 49/1999, FJ 6).

¹²⁹ El correo electrónico lleva aparejada de por sí la transmisión de la dirección IP, por lo que su utilización puede ser fuente de información personal identificable. Además, el carácter nominativo de la dirección de correo resulta obvia en tanto que el propio mensaje incorpora un campo que identifica al emisor del mensaje. Se podría, entonces, equiparar con la dirección del remitente de un mensaje ordinario (Corripio Delgado-Gil, 2000: 69).

¹³⁰ Recomendación 3/97 sobre el anonimato en Internet adoptada por el Grupo de trabajo el 3 de diciembre de 1997. XV D/5022/97 ES final WP6.

remitente de la misma comunicación, también los servicios tradicionales de telefonía ofrecen un mayor grado de anonimato que el correo electrónico dada la amplia disponibilidad de cabinas públicas que permiten acceder a la red de forma anónima, de manera que las llamadas efectuadas por este sistema no crea datos transaccionales identificables; este equilibrio alcanzado en otras tecnologías deberá preservarse en lo que respecta a los servicios ofrecidos a través de Internet. Para mantener este mismo nivel de protección resulta necesario arbitrar sistemas técnicos que permitan el anonimato en el correo electrónico (Corripio Delgado-Gil, 2000: 69-70).

Este derecho se engloba dentro de los derechos comunes a la protección de la intimidad personal y familiar, y se podría llegar a pensar que en realidad los apartados del art. 18 CE, son las distintas facetas del derecho a la intimidad. Sin embargo, el secreto a las comunicaciones –como el derecho a la autodeterminación informativa–, debe resultar protegido con independencia de su contenido, esto es, ya se trate de comunicaciones de carácter íntimo o de otro género, e incluso aunque no se trate de conocer el contenido de la comunicación (Perales, 2007: 15-16). El derecho al secreto de las comunicaciones puede imponer a los poderes públicos dos tipos de obligaciones: una negativa, la de abstenerse de interferir activamente con su ejercicio, y una positiva, la de procurar la eficacia efectiva del derecho (Rodríguez Ruiz, 1998: 80)¹³¹.

Es evidente también, apunta Morales (1995: 46) que la comunicación, cuya interceptación prohíbe la Constitución, es la realizada sin publicidad, la no susceptible, por su propia naturaleza, de ser conocida por terceros. Además señala que, lo que el artículo 18.3 CE protege no es el hecho técnico de la comunicación, sino el derecho a la autodeterminación del individuo en ese ámbito. Por lo tanto,

¹³¹ Los sujetos titulares del derecho al secreto de las comunicaciones son los comunicantes. Así en la correspondencia epistolar se distinguen tres derechos: a) el derecho a la propiedad material, que corresponde al destinatario; b) el derecho de autor, que corresponde al remitente y c) el derecho al secreto, que corresponde tanto al remitente como al destinatario. En tanto que en llamadas telefónicas, lo son quienes se comunican y no los titulares de las líneas telefónicas por las cuales se realiza la comunicación. En el caso de intervenciones telefónicas o de correspondencia, pueden existir terceros afectados, que comprenden aquel círculo de personas relacionadas con quien es sujeto de la medida de interceptación, que como es en el caso de las comunicaciones telefónicas, puede darse que, un mismo aparato, sea utilizado por varias personas, algunas de ellas indeterminadas (Saez Capel, 1999: 69-71). Al respecto del derecho al secreto de las comunicaciones y sus límites véase a Corripio Gil-Delgado y Marroig Pol (2001: 103-108).

no entraría dentro del concepto constitucional de comunicación, lógicamente, la carta abierta publicada en un diario, pues la misma no está sino destinada a que muchas personas la lean y a crear un estado de opinión.

En este sentido, es interesante cómo el derecho al secreto de las telecomunicaciones guarda un importante parecido con el derecho a la protección de datos personales, ambos tienden a ser protegidos independientemente de su contenido¹³². En otras palabras, la información manejada tanto en la comunicación como en la base de datos, sea o no información privada, deberá ser garantizada por el Estado, con la finalidad de salvaguardar un adecuado desenvolvimiento del individuo, a fin que no sea conocido por terceras personas, lo que él no ha destinado a la publicidad.

1.4 Límite al uso de la informática para garantizar el honor y la intimidad personal y familiar.

El artículo 18.4 CE, regula en definitiva el derecho a la protección de datos personales, al establecer que la Ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos, así como el pleno ejercicio de sus derechos. Lo que pretende el legislador es garantizar el honor y la intimidad, a través de la restricción en el uso de medios informáticos, que para 1978 era un paso bastante significativo, principalmente por no formar parte de la vida diaria en la sociedad y por el avance tecnológico que no es comparable con el de hoy en día. Actualmente, dicho precepto ha sido desarrollado por la Ley de la materia aplicable, así como por distintos instrumentos internacionales.

2. Evolución de la Jurisprudencia del Tribunal Constitucional en la configuración del derecho a la protección de datos.

Tradicionalmente, y como se ha apuntado con antelación, el derecho protegido había sido el derecho a la privacidad, y así es reflejado en las primeras Sentencias del Tribunal Constitucional de España. Dichas resoluciones resuelven

¹³² Para mayor abundamiento en el tema de protección de datos personales en las telecomunicaciones véase: Messía de la Cerda Ballesteros (2004: 13-84)

conflictos derivados de la vulneración del derecho a la intimidad, que suponían el acceso por parte de terceros a los datos de carácter personal que habían sido objeto de tratamiento informático. Así también veremos, como el derecho a la intimidad se va quedando de lado frente a casos particulares, para aparecer y reconocer lo que hoy en día es el derecho a la protección de datos personales.

2.1 STC 110/1984

En este caso el recurrente alegaba que mediante la intromisión de la autoridad fiscal en las cuentas sometidas a investigación, además de vulnerar su derecho a la intimidad arrojaría datos que revelarían su “biografía personal en números”¹³³. La Sentencia reconoce que el avance de la tecnología y el desarrollo de los medios de comunicación de masas, ha obligado a extender la protección de la vida privada más allá de los límites tradicionales, como el domicilio y la correspondencia¹³⁴, que de forma continuada han sido garantizados por los instrumentos internacionales de derechos humanos. Y admite la necesidad de redefinir el derecho a la privacidad y su interpretación, para hacer frente a los cambios tecnológicos que la propia sociedad estaba desarrollando.

Esta Sentencia acepta que los datos de carácter económico forman parte de la intimidad de la persona, con la reserva, en el caso examinado, en favor de la Hacienda Pública, pero la protección constitucional de la reserva de esos datos económicos como «íntimos», está en función de la protección de la privacidad, que es también protección de la libertad y de las posibilidades de autorrealización del individuo (FJ 8).

¹³³ Se solicitaba la anulación de una resolución de la Dirección General de la Inspección Financiera y Tributaria que autorizaba la investigación de las operaciones activas y pasivas del recurrente en amparo, en determinadas entidades bancarias y de crédito. El recurrente alegaba que la mencionada resolución vulneraba su derecho a la intimidad personal y familiar.

¹³⁴ La STC 110/1984, FJ 3, cuando refiere el ámbito de la intimidad establece que el “avance de la tecnología actual y el desarrollo de los medios de comunicación de masas ha obligado a extender esa protección más allá del aseguramiento del domicilio como espacio físico en que normalmente se desenvuelve la intimidad y del respeto a la correspondencia, que es o puede ser medio de conocimiento de aspectos de la vida privada. De aquí el reconocimiento global de un derecho a la intimidad o a la vida privada que abarque las intromisiones que por cualquier medio puedan realizarse en ese ámbito reservado de vida. No siempre es fácil, sin embargo, acotar con nitidez el contenido de la intimidad”.

2.2 STC 142/1993

En la STC 142/1993¹³⁵ –casi diez años después de la STC 110/1984– se admite el peligro que podría suponer para la intimidad el tratamiento de datos personales con una finalidad distinta de aquella para la que habían sido recogidos, aunque esto lo hace siguiendo la línea de argumentación desde el punto de vista de la intimidad¹³⁶. Este fallo reafirma la doctrina de la STC 110/1984, en la que se advierte la posibilidad de que en una sociedad tecnológicamente avanzada, el estudio de los datos financieros de una persona, puedan llegar a reconstruir el desarrollo de su vida íntima.

En esta Sentencia el Abogado del Estado reflexiona sobre la importancia de garantizar la capacidad de cada persona para controlar la propia información, y aduce que la intimidad del art. 18.1 CE debe interpretarse de manera que comprenda todo lo concerniente a la vida privada (FJ 2). El control sobre el flujo de información es “parte sustancial del derecho a moldear el yo que cada uno presenta ante el mundo y en razón del cual el mundo a su vez moldea la existencia de cada uno”¹³⁷.

La Sentencia recuerda también la doctrina sobre la intimidad de la STC 170/1987, cuando refiere que el atributo más importante de ésta, como núcleo central de la personalidad, es la facultad de exclusión de los demás, de abstención de injerencias por parte de otro, tanto en lo que se refiere a la toma de conocimientos intrusiva, como a la divulgación ilegítima de esos datos. La conexión de la intimidad con la libertad y dignidad de la persona, implica que la esfera de la inviolabilidad del individuo frente a injerencias externas en el ámbito personal y familiar, sólo en ocasiones tenga proyección hacia el exterior. Por lo

¹³⁵ Recurso de Inconstitucionalidad contra la Ley 2/1991, de 7 de enero, sobre derechos de información de los representantes de los trabajadores en materia de contratación. A juicio del recurrente, la referida ley vulneraba el derecho a la intimidad personal “económica” porque obligaba a los empresarios a entregar a los representantes de los trabajadores una copia básica de los contratos que debían celebrarse por escrito.

¹³⁶ “Lo decisivo para determinar la licitud o ilicitud de esta circulación no es un incondicionado y absoluto derecho a la preservación de la reserva sobre los datos económicos sino la aptitud de estos para, en un análisis detallado y conjunto, acceder a informaciones ya no atinentes a la esfera económica de la persona sino relativas directamente a su vida íntima personal y familiar”, conforme al FJ 8 de la STC 142/1993, hablando de la circulación de datos.

¹³⁷ STC 142/1993, antecedente 6 II.c.

que no comprende en principio los hechos referidos a las relaciones sociales y profesionales en que se desarrolla la actividad laboral, que están más allá del ámbito del espacio de intimidad personal y familiar sustraído a intromisiones extrañas por formar parte del ámbito de la vida privada (FJ 7).

Las retribuciones que el trabajador obtiene de su trabajo no pueden en principio desgajarse de la esfera de las relaciones sociales y profesionales que el trabajador desarrolla fuera de su ámbito personal e íntimo, para introducirse en este último, y hay que descartar que el conocimiento de la retribución percibida permita reconstruir la vida íntima de los trabajadores (FJ 8).

2.3 STC 254/1993

El Tribunal en este mismo año (1993) cuando ya hablaba del tratamiento de datos personales, dicta una nueva Sentencia en la que refiere por primera vez la “libertad informática”¹³⁸. En ésta recuerda que el Consejo de Europa refuerza la protección del derecho a la protección de datos personales de los ciudadanos, por la creciente utilización de la informática para fines administrativos y de gestión; lo que da lugar a que, en la sociedad moderna, gran parte de las decisiones que afectan a los individuos descansan en datos registrados en ficheros automatizados (FJ 4).

Según la Sentencia se reconocen dos aspectos del derecho a la intimidad, el negativo y el positivo (FJ 7). El negativo, se percibe en el límite del uso de la informática, siendo éste aquel que se encuentra en el respeto al honor y la intimidad de las personas y en el pleno ejercicio de sus derechos; y el positivo, refiere que la garantía de la intimidad se adopta hoy, en forma de derecho de control sobre los datos relativos a la propia persona.

La libertad informática, se configura como el aspecto positivo del derecho a la intimidad, es decir, el derecho a controlar el uso de los datos personales insertos en un programa informático, es decir, lo que se da por denominar habeas

¹³⁸ Recurso de Amparo interpuesto en contra de una negación (denegada por silencio Administrativo) por parte del Gobernador Civil a suministrar al recurrente, la información de los datos personales del mismo, que obraban en ficheros automatizados de la Administración del Estado.

data (FJ 7). El ejercicio del derecho a la intimidad justifica que, en algunos casos, el ciudadano se niegue a suministrar ciertos datos personales a la autoridad. Así mismo, aquél podrá oponerse a que dicha información sea conservada una vez cumplido el fin por el cual fue recabada. Podrá resistirse además, a que sus datos sean utilizados o difundidos para fines distintos, y aun ilegales o fraudulentos, o incluso que esos datos personales que tiene derecho a negar a la Administración sean suministrados por terceros no autorizados para ello.

Es preciso aclarar que el habeas data es una garantía para asegurar la libertad, y no solo habrá de concebirse como un procedimiento de protección de la intimidad (Serrano Pérez, 2003: 75). Esta libertad no es otra que el propio contenido del derecho a la autodeterminación informativa, el cual no es otra cosa que el derecho del individuo a que los demás sepan de él sólo lo que él desea que se sepa, así como el derecho a conocer los datos propios que figuren en ficheros ajenos (Del Castillo Vázquez, 2007: 139).

La Sentencia admite que la creación del Registro General de Protección de Datos, y el establecimiento de la Agencia de Protección de Datos, facilitan y garantizan el ejercicio de los derechos de información y acceso de los ciudadanos a los ficheros de titularidad pública, y además extienden su alcance a los ficheros de titularidad privada (FJ 8). Y entiende que la libertad informática puede ser el germen de un nuevo derecho constitucional, como derecho a controlar los propios datos, aunque todavía la doctrina del propio Tribunal no termina por desvincularlo del derecho fundamental a la intimidad¹³⁹.

En su FJ 6, establece, refiriéndose al art. 18.4 de la CE, que:

“De este modo, nuestra Constitución ha incorporado una nueva garantía constitucional, como forma de respuesta a una nueva forma de amenaza concreta

¹³⁹ “Esta constatación elemental de que los datos personales que almacena la Administración son utilizados por sus autoridades y sus servicios impide aceptar la tesis de que el derecho fundamental a la intimidad agota su contenido en facultades puramente negativas, de exclusión. Las facultades precisas para conocer la existencia, los fines y los responsables de los ficheros automatizados dependientes de una Administración pública donde obran datos personales de un ciudadano son absolutamente necesarias para que los intereses protegidos por el art. 18 CE, y que dan vida al derecho fundamental a la intimidad, resulten real y efectivamente protegidos. Por ende, dichas facultades de información forman parte del contenido del derecho a la intimidad, que vincula directamente a todos los poderes públicos, y ha de ser salvaguardado por este Tribunal, haya sido o no desarrollado legislativamente” (STC 254/1993, FJ 7).

a la dignidad y a los derechos de la persona, de forma en último término no muy diferente a como fueron originándose e incorporándose históricamente los distintos derechos fundamentales. En el presente caso estamos ante un instituto de garantía de otros derechos, fundamentalmente el honor y la intimidad, pero también de un instituto que es, en sí mismo, un derecho o libertad fundamental, el derecho a la libertad frente a las potenciales agresiones a la dignidad y a la libertad de la persona provenientes de un uso ilegítimo del tratamiento mecanizado de datos, lo que la Constitución llama «la informática».

En este orden de ideas, y como se ha referido el contenido del FJ 7, la Sentencia reconoce “un derecho a controlar el uso de los mismos datos insertos en un programa informático”. Es así que el Tribunal, se perfila y avanza en la construcción de este nuevo derecho fundamental al que progresivamente va desvinculando del derecho a la intimidad. Así lo refleja el Tribunal en su STC 11/1998¹⁴⁰ al referir que el art. 18.4 de la CE “no sólo entraña un específico instrumento de protección de los derechos del ciudadano frente al uso torticero de la tecnología informática, como ha quedado dicho, sino que además, consagra un derecho fundamental autónomo a controlar el flujo de informaciones que conciernen a cada persona (...) pertenezcan o no al ámbito más estricto de la intimidad, para así preservar el pleno ejercicio de sus derechos”¹⁴¹.

Sin embargo, Gómez Navajas (2005: 123) dice que en esta sentencia el Tribunal incurre en una contradicción al afirmar que, por un lado, la informática trata de tutelar derechos fundamentales ya reconocidos y señala, por otro, la sustantividad de un derecho en este ámbito.

2.4 STC 144/1999

Esta Sentencia es producto de un hecho por demás peculiar, en el que una Junta Electoral, de modo irregular, solicita vía telefónica al Registro Central de Penados y Rebeldes, la hoja histórico-penal; y su remisión por fax, sin que el Registro haya adoptado precaución alguna. La evidente vulneración de la intimidad, es producto de la cesión de los datos personales, considerados dentro

¹⁴⁰ En donde el recurrente demandaba su derecho a la libertad sindical.

¹⁴¹ SSTC 11/1998, FJ 5; 94/1998, FJ 4.

de la esfera más íntima, como es el historial penal de un individuo, sin previo conocimiento y consentimiento de su titular.

La Sentencia, establece que del art. 18.1 CE se deduce que el derecho a la intimidad garantiza al individuo un poder jurídico sobre la información relativa a su persona o familia, pudiendo imponer a terceros, sean estos simples particulares o poderes públicos, su voluntad de no dar a conocer dicha información o prohibiendo su difusión no consentida (FJ 8).

Llegados a este punto, es importante destacar que todas las Sentencias que se han precisado y posteriores a la STC 254/1993, inciden en un nuevo derecho, que se puede traducir en el derecho de la persona a controlar su información personal, y se perfila así, como un derecho distinto a la intimidad. A la vez, que se configura con un carácter instrumental para poder hacer efectivos otros derechos de la persona¹⁴², que no podrían garantizarse sin el reconocimiento del derecho a la protección de datos, que deviene de esta manera en derecho fundamental.

2.5 STC 290/2000

En esta Sentencia se examina la disputa competencial de las Comunidades Autónomas con la Agencia de Protección de Datos, partiendo de dos presupuestos, a saber¹⁴³:

- 1) El contenido del derecho fundamental a la protección de datos personales, y;
- 2) Los rasgos generales que caracterizan a la Agencia de Protección de Datos, ya que la función general de este órgano es velar por el cumplimiento de la legislación sobre protección de datos y controlar su aplicación.

¹⁴² La protección de datos personales deviene como un derecho imprescindible para garantizar la protección de la dignidad de la persona, los derechos inviolables que le son inherentes y el libre desarrollo de la personalidad, en un mundo dominado por el uso de las tecnologías informáticas.

¹⁴³ La Sentencia resuelve un Recurso de Inconstitucionalidad contra ciertos preceptos de la derogada LORTAD.

En lo que corresponde al primero, el Tribunal señala que el art. 1 LORTAD establece que el objeto de la Ley es el desarrollo de lo previsto en el art. 18.4 CE, y que contiene un instituto de garantía de los derechos a la intimidad y al honor, así como del pleno disfrute de los demás derechos de los ciudadanos y que es, además, en sí mismo, “un derecho fundamental, el derecho a la libertad frente a las potenciales agresiones a la dignidad y a la libertad de la persona provenientes de un uso ilegítimo del tratamiento automatizado de datos, lo que la Constitución llama «la informática»”¹⁴⁴.

El desarrollo del art. 18.4 CE dentro de las previsiones de la LORTAD, se centra en limitar principalmente el uso de la informática, ya que está directamente vinculada a la salvaguardia del derecho fundamental a la protección de datos personales, también llamado “libertad informática”¹⁴⁵. Y recuerda –lo dicho antes– el aspecto institucional de tales previsiones al señalar que, tras la aprobación de la LORTAD, la creación del Registro General de Protección de Datos y el establecimiento de la Agencia de Protección de Datos, facilitarán y garantizarán el ejercicio de los derechos de información y acceso de los ciudadanos a los ficheros de titularidad pública, extendiéndose además su alcance a los de titularidad privada¹⁴⁶.

De la lectura de esta Sentencia, se desprende indudablemente que el Tribunal se decanta por el reconocimiento de la protección de datos personales como un derecho fundamental, definiéndolo como aquel que garantiza a la persona un poder de control y disposición sobre sus datos personales. Pues confiere a su titular un haz de facultades que son elementos esenciales de este derecho, integrado por la potestad que corresponde al afectado de consentir la recogida y uso de sus datos personales, y a conocer los mismos. Y para hacer efectivo ese contenido, el derecho a ser informado de quién posee sus datos y con qué finalidad, así como el derecho a oponerse a esa posesión y uso, exigiendo a quien corresponda que ponga fin a la misma, así como al empleo de dicha información.

¹⁴⁴ FJ 7. Doctrina de las SSTC 254/1993, FJ 6; 143/1994, FJ 7; 11/1998, FJ 4; 94/1998, FJ 6 y 202/1999, FJ 2.

¹⁴⁵ Expresión utilizada por la STC 254/1993.

¹⁴⁶ STC 254/1993, FJ 10.

En suma, este nuevo derecho fundamental comprende un conjunto de derechos que el ciudadano puede ejercer frente a quienes sean titulares, públicos o privados, de ficheros de datos personales, partiendo del conocimiento de tales ficheros y de su contenido, uso y destino, por el registro de los mismos. De suerte que es sobre dichos ficheros donde han de proyectarse, en última instancia, las medidas destinadas a la salvaguardia del derecho fundamental aquí considerado por parte de las Administraciones Públicas competentes (FJ 7).

La idea de la configuración, de la protección de datos personales, como un derecho autónomo distinto del de intimidad, es desarrollada también por el voto particular de esta Sentencia¹⁴⁷. Este señala que se debió afirmar de modo explícito en la argumentación del fallo, que el Tribunal estaba reconociendo y protegiendo desde ese momento un nuevo derecho fundamental, el derecho de libertad informática, que no figuraba en la Tabla del texto de 1978. Voto particular, que amén de la importancia que tiene de cara a subrayar el nacimiento de un nuevo derecho fundamental de creación jurisprudencial, que es el derecho fundamental a la protección de datos personales o libertad informática, abre las puertas al reconocimiento de nuevos derechos fundamentales por la Jurisprudencia del Tribunal Constitucional¹⁴⁸.

2.6 STC 292/2000

En esta Sentencia se consolida la denominación de derecho a la protección de datos personales en sustitución de libertad informática –que el Tribunal venía utilizando–, y le otorga el carácter de derecho fundamental. Cuyo contenido, se ha dicho antes, es el control sobre los propios datos, que se traduce en el haz de facultades necesario para que el citado control resulte verdaderamente efectivo, y que deviene como un derecho imprescindible para garantizar la protección de la dignidad de la persona, los derechos inviolables que le son inherentes y el libre

¹⁴⁷ Único voto particular en la Sentencia, presentado por el Magistrado Manuel Jiménez de Parga y Cabrera, y al que se adhirió el Magistrado Rafael de Mendizábal Allende.

¹⁴⁸ Cuestión de enorme interés que sería materia suficiente para una monografía, pero que no es objeto de estudio en el presente trabajo. Hemos de mencionar también que el voto particular hace derivar la libertad informática no sólo del art. 18.4 CE, sino sobre todo del art. 10.1 CE, en cuanto el reconocimiento del citado derecho es necesario para garantizar la dignidad de la persona, los derechos inviolables que le son inherentes y el libre desarrollo de la personalidad.

desarrollo de la personalidad, en un mundo dominado por el uso de las tecnologías informáticas.

La Sentencia sostiene que el derecho fundamental a la protección de datos personales, es en sí mismo un derecho o libertad fundamental, es decir, el derecho a la libertad frente a las potenciales agresiones a la dignidad y a la libertad de la persona, provenientes de un uso ilegítimo del tratamiento mecanizado de datos, lo que la Constitución llama «la informática», y lo que se ha dado en llamar “libertad informática” (FJ 5). El Tribunal, además, refiere que este derecho contiene un instituto de garantía de los derechos a la intimidad, al honor y al pleno disfrute de los restantes derechos de los ciudadanos, por ello se dice que es en sí mismo un derecho fundamental¹⁴⁹.

La garantía de la vida privada de la persona y de su reputación poseen hoy una dimensión positiva que excede el ámbito propio del derecho fundamental a la intimidad (art. 18.1 CE), y que se traduce en un derecho de control sobre los datos relativos a la propia persona. La llamada "libertad informática" es el derecho a controlar el uso de los datos insertos en un programa informático (habeas data) y comprende, entre otros aspectos, la oposición del ciudadano a que determinados datos personales sean utilizados para fines distintos de aquel legítimo que justificó su obtención (SSTC 11/1998, FJ 5 y 94/1998, FJ 4) (FJ 5).

El fallo distingue el derecho fundamental a la protección de datos personales del derecho a la intimidad. Ambos comparten el objetivo de ofrecer una eficaz protección constitucional de la vida personal y familiar, atribuyendo a

¹⁴⁹ Este fallo contiene un recuento interesante de las Sentencias relacionadas con el art. 18.4 CE, y refiere que éste fue esgrimido por primera vez en el caso de un ciudadano a quien el Gobierno Civil de Guipúzcoa le denegó información sobre los datos que sobre su persona poseía, resuelto por la STC 254/1993. Y lo dicho en esta Sentencia pionera se fue aquilatando en las posteriores, como la relativa a las normas reguladoras del número de identificación fiscal (STC 143/1994), o la que declaró contrario a la libertad sindical (art. 28 CE), en relación con el art. 18.4 CE, el uso por una empresa del dato de la afiliación sindical para detraer haberes de los trabajadores con ocasión de una huelga promovida por determinado sindicato, STC 11/1998 (cuya doctrina ha sido reiterada en una larga serie de Sentencias de este Tribunal resolviendo idéntica cuestión, y de entre las que merece destacarse la STC 94/1998), o, finalmente y hasta la fecha, la STC 202/1999 en la que, con ocasión de la denegación a un trabajador de la cancelación de sus datos médicos en un fichero informatizado de una entidad de crédito sobre bajas por incapacidad temporal, se apreció que el almacenamiento sin cobertura legal en soporte informático de los diagnósticos médicos del trabajador sin mediar su consentimiento expreso constituía una desproporcionada restricción del derecho fundamental a la protección de datos personales (FJ 5).

su titular un haz de facultades consistentes, predominantemente, en el poder jurídico de imponer a terceros la realización u omisión de determinada conducta (cuya concreta regulación debe establecer la Ley), principalmente aquella que conforme al art. 18.4 CE debe limitar el uso de la informática, bien desarrollando el derecho fundamental a la protección de datos (art. 81.1 CE), bien regulando su ejercicio (art. 53.1 CE). La peculiaridad del derecho a la protección de datos respecto de la intimidad, radica en su distinta función, que apareja por consiguiente que también su objeto y contenido difieran (FJ 5).

La Sentencia establece de manera definitiva que el derecho a la protección de datos es un derecho autónomo y diferenciado del derecho a la intimidad, ya que ambos poseen diferencias tanto en su función, como de objeto y contenido.

La principal divergencia entre ambos radica esencialmente en su función y la desglosa así:

El derecho a la Intimidad tiene la función de proteger, frente a cualquier invasión que pueda realizarse en el ámbito de la vida personal y familiar, aquella información que la persona desea excluir del conocimiento ajeno y de las intromisiones de terceros en contra de su voluntad. Permite excluir ciertos datos de una persona del conocimiento ajeno, es decir, el poder de resguardar su vida privada de una publicidad no deseada.

El derecho de protección de datos, persigue garantizar a la persona, un poder de control sobre sus datos personales, su uso y destino, con el propósito de impedir su tráfico ilícito y lesivo para la dignidad y derecho del afectado. Este derecho garantiza a los individuos un poder de disposición sobre esos datos. Esta garantía impone a los poderes públicos la prohibición de que se conviertan en fuente de esa información sin las debidas garantías, y también el deber de prevenir los riesgos que puedan derivarse del acceso o divulgación indebida de dicha información. Sin embargo, es de destacar que, ese poder de disposición sobre los propios datos personales de nada sirve, si el afectado desconoce cuáles datos de sí mismo se encuentran en posesión de terceros, quiénes los poseen, y con qué fin están en poder de estos.

En cuanto al objeto de ambos derechos, enlazando con la diferente función de los mismos, la Sentencia dice que la singularidad del derecho a la protección de datos, es un objeto más amplio, comparado con el derecho a la intimidad¹⁵⁰. La protección de datos extiende su garantía no sólo a la intimidad en su dimensión constitucionalmente protegida por el art. 18.1 CE, sino a lo que en ocasiones el Tribunal ha definido en términos más amplios, como la esfera de los bienes de la personalidad que pertenecen al ámbito de la vida privada, inconfundiblemente unidos al respeto de la dignidad personal¹⁵¹, como el derecho al honor, citado expresamente en el art. 18.4 CE, e igualmente, en expresión bien amplia del propio art. 18.4 CE, al pleno ejercicio de los derechos de la persona. El derecho fundamental a la protección de datos amplía la garantía constitucional a aquellos datos que sean relevantes para o tengan incidencia en el ejercicio de cualesquiera derechos de la persona, sean o no derechos constitucionales y sean o no relativos al honor, la ideología, la intimidad personal y familiar, y a cualquier otro bien constitucionalmente amparado¹⁵².

Es de destacar que el objeto de protección del derecho fundamental a la protección de datos no se reduce sólo a los datos íntimos de la persona, sino 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 sólo la intimidad individual, pues para ello está la protección que el art. 18.1 CE otorga, sino los datos de carácter personal¹⁵³.

Por consiguiente, también alcanza a aquellos datos personales públicos, que por el hecho de serlo, de ser accesibles al conocimiento de cualquiera, no escapan al poder de disposición del afectado porque así lo garantiza su derecho a la protección de datos. También por ello, el que los datos sean de carácter personal no significa que sólo tengan protección los relativos a la vida privada o íntima de la persona, sino que los datos amparados son todos aquellos que identifiquen o permitan la identificación de la persona, pudiendo servir para la confección de su perfil ideológico, racial, sexual, económico o de cualquier otra

¹⁵⁰ STC 292/2000, FJ 6.

¹⁵¹ STC 170/1987, FJ 4

¹⁵² STC 292/2000, FJ 5.

¹⁵³ STC 292/2000, FJ 6.

índole, o que sirvan para cualquier otra utilidad que en determinadas circunstancias constituya una amenaza para el individuo¹⁵⁴.

Finalmente, en cuanto al distinto contenido de ambos derechos, la Sentencia precisa que “el derecho fundamental a la protección de datos posee una segunda peculiaridad que lo distingue de otros, como el derecho a la intimidad personal y familiar del art. 18.1 CE. Dicha peculiaridad radica en su contenido, ya que a diferencia de este último, que confiere a la persona el poder jurídico de imponer a terceros el deber de abstenerse de toda intromisión en la esfera íntima de la persona y la prohibición de hacer uso de lo así conocido. El derecho a la protección de datos atribuye a su titular un haz de facultades consistente en diversos poderes jurídicos cuyo ejercicio impone a terceros deberes jurídicos, que no se contienen en el derecho fundamental a la intimidad, y que sirven a la capital función que desempeña este derecho fundamental: garantizar a la persona un poder de control sobre sus datos personales, lo que sólo es posible y efectivo imponiendo a terceros los mencionados deberes de hacer. A saber: el derecho a que se requiera el previo consentimiento para la recogida y uso de los datos personales, el derecho a saber y ser informado sobre el destino y uso de esos datos y el derecho a acceder, rectificar y cancelar dichos datos. En definitiva, el poder de disposición sobre los datos personales”¹⁵⁵.

3. Derecho de Protección de Datos Personales

La STC 292/2000 distingue el derecho fundamental a la protección de datos personales del derecho a la intimidad. Ambos comparten el objetivo de ofrecer una eficaz protección constitucional de la vida personal y familiar, atribuyendo a su titular un haz de facultades consistentes, predominantemente, en el poder jurídico de imponer a terceros la realización u omisión de determinada conducta (cuya concreta regulación debe establecer la Ley), principalmente aquella que conforme al art. 18.4 CE debe limitar el uso de la informática, bien desarrollando el derecho fundamental a la protección de datos (art. 81.1 CE), bien regulando su ejercicio (art. 53.1 CE). La peculiaridad del derecho a la protección

¹⁵⁴ *Idem.*

¹⁵⁵ *Idem.*

de datos respecto de la intimidad, radica en su distinta función, que apareja por consiguiente que también su objeto y contenido difieran¹⁵⁶

Esta Sentencia establece de manera definitiva que el derecho a la protección de datos es un derecho autónomo y diferenciado del derecho a la intimidad, ya que ambos poseen diferencias tanto en su función, como de objeto y contenido, mismos que se verán diferenciados en los epígrafes que vienen a continuación.

3.1 Objetivo

Es de destacar que el objeto de protección del derecho fundamental a la protección de datos no se reduce sólo a los datos íntimos de la persona, sino 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 sólo la intimidad individual, que para ello está la protección que el art. 18.1 CE otorga, sino los datos de carácter personal¹⁵⁷.

Por consiguiente, también alcanza a aquellos datos personales públicos, que por el hecho de serlo, de ser accesibles al conocimiento de cualquiera, no escapan al poder de disposición del afectado porque así lo garantiza su derecho a la protección de datos. También por ello, el que los datos sean de carácter personal no significa que sólo tengan protección los relativos a la vida privada o íntima de la persona, sino que los datos amparados son todos aquellos que identifiquen o permitan la identificación de la persona, pudiendo servir para la confección de su perfil ideológico, racial, sexual, económico o de cualquier otra

¹⁵⁶ STC 292/2000, FJ 5.

¹⁵⁷ STC 292/2000, FJ 6. Por otro lado, La STC 292/2000 también dice que la singularidad del derecho a la protección de datos, es por un lado, su objeto que es más amplio, comparado con el derecho a la intimidad¹⁵⁷. La protección de datos extiende su garantía no sólo a la intimidad en su dimensión constitucionalmente protegida por el art. 18.1 CE, sino a lo que en ocasiones el Tribunal ha definido en términos más amplios, como la esfera de los bienes de la personalidad que pertenecen al ámbito de la vida privada, confusamente unidos al respeto de la dignidad personal, como el derecho al honor, citado expresamente en el art. 18.4 CE, e igualmente, en expresión bien amplia del propio art. 18.4 CE, al pleno ejercicio de los derechos de la persona. El derecho fundamental a la protección de datos amplía la garantía constitucional a aquellos datos que sean relevantes para o tengan incidencia en el ejercicio de cualesquiera derechos de la persona, sean o no derechos constitucionales y sean o no relativos al honor, la ideología, la intimidad personal y familiar, y a cualquier otro bien constitucionalmente amparado.

índole, o que sirvan para cualquier otra utilidad que en determinadas circunstancias constituya una amenaza para el individuo¹⁵⁸.

La finalidad de un sistema de protección de datos personales no es asegurar la opacidad de los datos relativos a una persona, para este fin está el derecho fundamental a la intimidad. Lo que el derecho a la protección de datos personales regula es el poder jurídico de disposición que la persona tiene sobre el uso y destino de sus datos, esto es, de su publicidad (Villaverde Menéndez, 2008: 265-266)¹⁵⁹.

3.2 Función

El derecho de protección de datos persigue garantizar a la persona un poder de control sobre sus datos personales, su uso y destino, con el propósito de impedir su tráfico ilícito y lesivo para la dignidad y derecho del afectado. Este derecho garantiza a los individuos un poder de disposición sobre esos datos. Esta garantía impone a los poderes públicos la prohibición de que se conviertan en fuente de esa información sin las debidas garantías, y también el deber de prevenir los riesgos que puedan derivarse del acceso o divulgación indebida de dicha información. Sin embargo, es de destacar que, ese poder de disposición sobre los propios datos personales de nada sirve, si el afectado desconoce cuáles

¹⁵⁸ STC 292/2000, FJ 6.

¹⁵⁹ Villaverde Menéndez (2008: 264) refiere que: “publicidad y datos personales son dos extremos en fricción al hablar de registros públicos. Estos tienen sentido como fuente de información que encuentra un límite de peso a su accesibilidad en la debida salvaguardia de los datos personales contenidos en sus asientos. Registros como el Civil, o el de Rebeldes Civiles, o el de Penados y Rebeldes, son ante todo datos personales reunidos y sistematizados para que quede constancia de nacimientos, fallecimientos, morosidades, ausencias, avatares vitales diversos, condenas y antecedentes penales. Otros, como el de Propiedad, pese a no ser su función primera ser fuente de información de datos relativos a personas, están ligados indefectiblemente a la circulación de esos datos que van unidos inevitablemente a aquellos que sí son objeto de ese registro en cuestión. No es baladí el asunto. Ocurre al tiempo que el registro cumple con esa primordial función, su publicidad, esto es, su accesibilidad general, produce efectos colaterales nada desdeñables y que, desde luego, deben tenerse muy en cuenta. El conocimiento que se alcanza con aquella publicidad registral conlleva inevitablemente la puesta a disposición de un tercero de datos de personas. Con ello, el registro, además, pone a disposición de quien accede a él datos de personas que pueden ser objeto de usos y destinos muy diversos. El acceso al registro permite identificar y también evaluar a una persona a través de los datos que obran en sus asientos, por lo que, y precisamente por ello, esos datos probablemente deban estar sujetos a un régimen jurídico peculiar y específico”.

datos de sí mismo se encuentran en posesión de terceros, quiénes los poseen, y con qué fin están en poder de estos¹⁶⁰.

3.3 Titulares

a) Personas físicas

La LOPD refiere que el objeto de aplicación de la misma, es únicamente para las personas físicas. En su artículo primero, se establece que la Ley Orgánica tiene 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. El art. 3 de la misma Ley, define al afectado o interesado como la persona física titular de los datos que sean objeto del tratamiento de datos.

En cuanto al consentimiento otorgado por los menores de edad, la AEPD considera que los mayores de catorce años disponen de las condiciones de madurez precisas para consentir, por sí mismos, el tratamiento automatizado de sus datos de carácter personal. Y que para los restantes menores de edad, no puede ofrecerse una solución claramente favorable a la posibilidad de que por los mismos pueda prestarse el consentimiento al tratamiento, por lo que deberá tomarse en cuenta, fundamentalmente, sus condiciones de madurez¹⁶¹.

b) Personas jurídicas

En España es interesante el ámbito de aplicación de la LOPD, ya que no se extiende a las personas jurídicas. El objeto de esta Ley está regulado en los arts. 1 y 2, y como se ha visto en el apartado anterior, la norma tiene por objeto

¹⁶⁰ La STC 292/2000 refiere que el derecho a la intimidad tiene la función de proteger, frente a cualquier invasión que pueda realizarse en el ámbito de la vida personal y familiar, aquella información que la persona desea excluir del conocimiento ajeno y de las intromisiones de terceros en contra de su voluntad. Permite excluir ciertos datos de una persona del conocimiento ajeno, es decir, el poder de resguardar su vida privada de una publicidad no deseada.

¹⁶¹ Informe de la AEPD 2000 0000 sobre consentimiento otorgado por menores de edad http://www.agpd.es/portalwebAGPD/canaldocumentacion/informes_juridicos/consentimiento/common/pdfs/2000-0000_Consentimiento-otorgado-por-menores-de-edad.pdf (consulta: 09/11/2012). Al respecto Arenas Ramiro (2006: 86) señala que los titulares del derecho reconocido en el art. 8 CEDH son, en primer lugar, las personas físicas; y que en la doctrina se plantearon dudas sobre la titularidad de los menores, pero el TEDH reconoció pronto la posibilidad de que fuesen titulares del derecho e incluso de que lo ejerciesen sin el consentimiento de su representante.

garantizar y proteger, en lo que concierne al tratamiento de datos personales de las personas físicas.

Sin embargo, a nivel europeo, en cuanto a las personas jurídicas, el TEDH reconoce la titularidad de los derechos recogidos en el CEDH a las personas jurídicas con ciertas matizaciones: sólo podrán ser titulares de aquellos derechos que por su propia naturaleza puedan disfrutar. En este sentido, el TEDH no les reconoce el derecho a la vida ni el derecho al respeto de la vida familiar, y no podrán alegar vida sexual, vida íntima o integridad corporal. Por el contrario, se ha admitido que podrán alegar la defensa de su derecho contra escuchas telefónicas y el respeto al domicilio o a la correspondencia, y por lo tanto el respeto a sus datos personales. En cualquier caso, no se reconoce que las autoridades públicas u otro tipo de organismos públicos puedan ser titulares de los derechos reconocidos en el CEDH (Arenas Ramiro, 2006: 87)¹⁶².

3.4 Contenido

El *contenido* del derecho a la protección de datos personales se encuentra en el art. 18.4 CE mismo que señala 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.

El Tribunal Constitucional señala que la LORTAD contiene un instituto de garantía de los derechos a la intimidad y al honor, que es en sí mismo, “un derecho fundamental, el derecho a la libertad frente a las potenciales agresiones a la dignidad y a la libertad de la persona provenientes de un uso ilegítimo del tratamiento automatizado de datos, lo que la Constitución llama «la informática»”¹⁶³.

¹⁶² Arenas Ramiro (2006: 87-88) refiere que en el caso de la protección de datos personales, titulares del derecho son todas las personas físicas y también las personas jurídicas. Aunque el TEDH no ha afirmado expresamente que las personas jurídicas sean titulares del derecho a la protección de datos, lo cierto es que ha resuelto diversos casos en que las personas jurídicas acudieron ante el Tribunal alegando la violación de su derecho a la protección de datos por el uso, almacenamiento y denegación de acceso de ciertos datos económicos o de personal relativos a esas personas jurídicas.

¹⁶³ FJ 7. Doctrina de las SSTC 254/1993, FJ 6; 143/1994, FJ 7; 11/1998, FJ 4; 94/1998, FJ 6 y 202/1999, FJ 2.

Este derecho fundamental comprende un conjunto de derechos que el ciudadano puede ejercer frente a quienes sean titulares, públicos o privados, de ficheros de datos personales, partiendo del conocimiento de tales ficheros y de su contenido, uso y destino, por el registro de los mismos¹⁶⁴.

La STC 292/2000 recuerda que el contenido de este derecho es el control sobre los propios datos, que se traduce en el haz de facultades necesario para que el citado control resulte verdaderamente efectivo, y que deviene como un derecho imprescindible para garantizar la protección de la dignidad de la persona, los derechos inviolables que le son inherentes y el libre desarrollo de la personalidad, en un mundo dominado por el uso de las tecnologías informáticas.

Finalmente, en cuanto contenido, la STC 292/2000 precisa que el derecho fundamental a la protección de datos posee una segunda peculiaridad que lo distingue de otros, como el derecho a la intimidad personal y familiar del art. 18.1 CE. Dicha peculiaridad radica en su contenido¹⁶⁵, que atribuye a su titular un haz de facultades consistente en diversos poderes jurídicos, cuyo ejercicio impone a terceros deberes jurídicos (que no se contienen en el derecho fundamental a la intimidad) y que sirven a la capital función que desempeña este derecho fundamental: garantizar a la persona un poder de control sobre sus datos personales, lo que sólo es posible y efectivo imponiendo a terceros los mencionados deberes de hacer. A saber: el derecho a que se requiera el previo consentimiento para la recogida y uso de los datos personales, el derecho a saber y ser informado sobre el destino y uso de esos datos y el derecho a acceder, rectificar y cancelar dichos datos. En definitiva, el poder de disposición sobre los datos personales¹⁶⁶.

¹⁶⁴ STC 290/2000, FJ 7.

¹⁶⁵ Ya que a diferencia de la protección de datos, el derecho a la intimidad confiere a la persona el poder jurídico de imponer a terceros el deber de abstenerse de toda intromisión en la esfera íntima de la persona y la prohibición de hacer uso de lo así conocido.

¹⁶⁶ STC 292/2000, FJ 6. Según Guichot (2009: 173) la doctrina del TC establece que dentro del contenido del derecho a la protección de datos se encuentran los principios de consentimiento, finalidad y exactitud, y los derechos a ser informado de los datos en poder de terceros, a acceder a ellos y a obtener su rectificación y cancelación en caso de incumplimiento de los principios mencionados.

3.5 Tipo de datos

La LOPD define a los datos de carácter personal como cualquier información concerniente a personas físicas identificadas o identificables. No es lo mismo un dato de ideología, raza, religión o vida sexual, que un dato de infracciones administrativas. La AEPD ha elaborado una Guía de Seguridad de Datos en la que precisa los tipos de datos, atendiendo a las medidas de seguridad exigibles a los ficheros y tratamientos de los mismos, clasificándolos en tres niveles acumulativos: básico, medio y alto. Esta clasificación se realiza atendiendo a la naturaleza de la información tratada, en relación con la menor o mayor necesidad de garantizar la confidencialidad y la integridad de la información. A continuación se indican los ficheros y tratamientos a los que corresponde aplicar las medidas de seguridad relativas a cada uno de los niveles que determina el art. 79 RD 1720/2007:

- a) Nivel alto. Ficheros o tratamientos con datos sensibles¹⁶⁷:
- De ideología, afiliación sindical, religión, creencias, origen racial, salud o vida sexual y respecto de los que no se prevea la posibilidad de adoptar el nivel básico.
 - Recabados con fines policiales sin consentimiento de las personas afectadas.
 - Derivados de actos de violencia de género.
- b) Nivel medio. Ficheros o tratamientos con datos:
- Relativos a la comisión de infracciones administrativas o penales.
 - Que se rijan por el artículo 29 de la LOPD (prestación de servicios de solvencia patrimonial y crédito).
 - De Administraciones tributarias, y que se relacionen con el ejercicio de sus potestades tributarias.

¹⁶⁷ Estos son los datos especialmente protegidos regulados por el art. 7 LOPD. La doctrina italiana refiere que para acceder a estos datos, principalmente en poder de la administración pública, se necesita de una disposición legal (Acciai, 2004: 439).

- De entidades financieras para las finalidades relacionadas con la prestación de servicios financieros.
 - De Entidades Gestoras y Servicios Comunes de Seguridad Social, que se relacionen con
 - el ejercicio de sus competencias;
 - De mutuas de accidentes de trabajo y enfermedades profesionales de la Seguridad Social;
 - Que ofrezcan una definición de la personalidad y permitan evaluar determinados aspectos de la misma o del comportamiento de las personas.
 - De los operadores de comunicaciones electrónicas, respecto de los datos de tráfico y localización¹⁶⁸.
- c) Nivel bajo. Cualquier otro fichero que contenga datos de carácter personal. También aquellos ficheros que contengan datos de ideología, afiliación sindical, religión, creencias, salud, origen racial o vida sexual, cuando:
- Los datos se utilicen con la única finalidad de realizar una transferencia dineraria a entidades de las que los afectados sean asociados o miembros.
 - Se trate de ficheros o tratamientos de estos tipos de datos de forma incidental o accesorio, que no guarden relación con la finalidad del fichero.
 - En los ficheros o tratamientos que contengan datos de salud, que se refieran exclusivamente al grado o condición de discapacidad o la simple declaración de invalidez, con motivo del cumplimiento de deberes públicos.

Respecto a los datos públicos, la doctrina italiana dice que son aquellos datos recolectados o utilizados por instituciones públicas en el ámbito de su actividad, por tanto, son aquellos de accesibilidad pública o que carecen de

¹⁶⁸ Para esta categoría de ficheros además deberá disponerse de un registro de accesos.

características para permanecer privados. En cuanto a esta definición se precisan algunas hipótesis que se pueden considerar al momento de clasificar un dato como público (Quaranta, 2005: 300 a 302): a) que no se pueda identificar al titular, es decir que sea anónimo, b) el origen de la información, por ejemplo, que provenga de un registro público, c) la desagregación y generalización de los datos para fines estadísticos, d) la forma de elaboración de los datos, que sean básicos para una estadística o bien enriquecidos, de tal forma que al conectarse no puedan identificar a una persona, y e) el uso que le dará a los datos el sujeto interesado.

El derecho a la autodeterminación informativa en España se encuentra regulado en la LOPD, y la titularidad de esta prerrogativa es para las personas físicas y no así para las jurídicas o morales.

3.6 Derechos de las personas

El derecho a la autodeterminación informativa en España se encuentra regulado en la LOPD, la titularidad de este derecho es para las personas físicas y jurídicas¹⁶⁹. El derecho a la protección de datos personales es muy peculiar dado que el mismo, comprende a su vez una serie de derechos en sí¹⁷⁰. En España, los derechos de las personas contenidos en la Ley son los siguientes¹⁷¹:

1. Derecho de impugnación de valoraciones
2. Derecho de consulta
3. Derecho de acceso
4. Derecho de rectificación y cancelación
5. Derecho de oposición
6. Derecho de indemnización
7. Derecho de reclamación y la tutela de los derechos

¹⁶⁹ La ley se desarrolla haciendo alusión a los ficheros de titularidad pública y/o privada.

¹⁷⁰ Véase: Fernández Delpech (2001: 220-222), Quiroga Lavié (2001: 96-106), Carranza Torres (2001: 89-108), Cesario (2001: 143-150) y Padilla (2001: 166-172).

¹⁷¹ Los derechos de las personas son conocidos como “derechos ARCO” porque comprenden el: acceso, rectificación, cancelación y oposición. Sin embargo, la Ley comprende otros derechos de las personas como el de información, impugnación de valoraciones, indemnización, reclamación, el de tutela de derechos, incluso el de gratuidad de algunos trámites, entre otros.

Como es natural, a estos derechos de los titulares de los datos personales, corresponden los correlativos deberes de quienes los acopian, tratan, transmiten, conservan o utilizan de cualquier manera (Murillo de la Cueva, 2000: 91).

3.6.1 Derecho a impugnación de valoraciones

El artículo 13 LOPD, vela por el derecho de la persona a la impugnación de valoraciones, dicho dispositivo está comprendido por cuatro numerales que son los siguientes:

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.

El dispositivo hace alusión a la obtención de perfiles personales, a través de la recolección de datos, que posteriormente podrían afectar el desarrollo de la vida privada del individuo¹⁷². La exposición de motivos de la LO 5/1992

¹⁷² El art. 36 RD 1720/2007, sobre el derecho de oposición a las decisiones basadas únicamente en un tratamiento automatizado de datos, refiere que los interesados 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 automatizado de datos destinado a evaluar determinados aspectos de su personalidad, tales como su rendimiento laboral, crédito, fiabilidad o conducta. No obstante, los afectados podrán verse sometidos a una de las decisiones descritas anteriormente,

(LORTAD), hace constar que la intimidad, en sentido estricto, está suficientemente protegida por las previsiones de los tres primeros párrafos del art. 18 CE y por las leyes que los desarrollan, sin embargo advierte que la privacidad puede resultar menoscabada por la utilización de las tecnologías informáticas de tan reciente desarrollo. Ello es así, porque hasta el presente, las fronteras de la privacidad estaban defendidas por el tiempo y el espacio. El primero procuraba, con su transcurso, que se evanescieran los recuerdos de las actividades ajenas, impidiendo así, la configuración de una historia lineal e ininterrumpida de la persona; el segundo, con la distancia que imponía, hasta hace poco difícilmente superable, impedía que tuviésemos conocimiento de los hechos que, protagonizados por los demás, hubieran tenido lugar lejos de donde nos hallábamos. El tiempo y el espacio operaban, así, como salvaguarda de la privacidad de la persona.

Dicha exposición de motivos, reconoce que uno y otro límite –del tiempo y el espacio– han desaparecido hoy. Las modernas técnicas de comunicación permiten salvar sin dificultades el espacio, y la informática posibilita almacenar todos los datos que se obtienen a través de las comunicaciones y acceder a ellos en apenas segundos, por distante que fuera el lugar donde transcurrieron los hechos, o remotos que fueran estos. Los más diversos datos sobre la infancia, sobre la vida académica, profesional o laboral, sobre los hábitos de vida y consumo, sobre el uso del denominado «dinero plástico» –transacciones con tarjetas bancarias–, sobre las relaciones personales o incluso sobre las creencias religiosas e ideologías. Lo anterior, solo por mencionar algunos ejemplos relativos a las personas, y que podrían así ser compilados y obtenidos sin dificultad. Ello permitiría a quien dispusiese de ellos, acceder a un conocimiento cabal de actitudes, hechos o pautas de comportamiento que, sin duda, pertenecen a la esfera privada de las personas. Ámbito privado al que sólo debe tener acceso el individuo y, quizás, quienes le son más próximos, o aquellos a los que él así

cuando la misma se haya adoptado en el marco de la celebración o ejecución de un contrato a petición el interesado, siempre que se le otorgue la posibilidad de alegar lo que estimara pertinente, a fin de defender su derecho o interés. En todo caso, el responsable del fichero deberá informar previamente al afectado, de forma clara y precisa, de que se adoptarán decisiones con las características señaladas en el apartado 1 y cancelará los datos en caso de que no llegue a celebrarse finalmente el contrato.

autorice. El conocimiento ordenado de esos datos puede dibujar un determinado perfil de la persona, o configurar una determinada reputación o fama que es, en definitiva, expresión del honor; y este perfil personal¹⁷³, sin duda, puede resultar luego valorado, favorable o desfavorablemente, para las más diversas actividades públicas o privadas, como pueden ser la obtención de un empleo, la concesión de un préstamo o la admisión en determinados colectivos.

Para la adecuada configuración, que la LO 15/1992 se propuso, de la nueva garantía de la intimidad y del honor, resultó esencial la correcta regulación de la cesión de los datos almacenados. Ya que es el cruce de los datos almacenados en diversas instancias o ficheros el que puede arrojar el aludido perfil personal, cuya obtención transgrediría los límites de la privacidad. Para prevenir estos perturbadores efectos, la Ley completó el principio del consentimiento, exigiendo que, al procederse a la recogida de los datos, el afectado fuese debidamente informado del uso que se les podría dar. Sólo las previsiones del Convenio Europeo para la protección de los Derechos Fundamentales de la Persona (art. 8.2) y del Convenio 108 del Consejo de Europa (art. 9.2), que se fundamentan en exigencias lógicas en toda sociedad democrática, constituyen excepciones a esta regla¹⁷⁴.

¹⁷³ A tal efecto, la exposición de motivos de la LO 15/1992, introduce y así lo cita, que el concepto de tratamiento de datos en ficheros (concibiéndolos desde una perspectiva dinámica) no los entiende sólo como un mero depósito de datos, sino también, y sobre todo, como una globalidad de procesos o aplicaciones informáticas que se llevan a cabo con los datos almacenados y que son susceptibles, si llegasen a conectarse entre sí, de configurar el *perfil persona*, que antes hemos referido.

¹⁷⁴ Las valoraciones son frecuentes, en los supuestos de *scoring* o establecimiento de riesgos de clientes, en dónde diversas instituciones intercambian datos, para rechazar o no la solicitud de un cliente, con relación, por ejemplo, a un crédito hipotecario. En este caso, tal prueba de *scoring* y el tratamiento de datos que implica ha de contar, inexcusablemente, con el consentimiento inequívoco e informado del afectado, que no puede acogerse a la excepción del art. 6.2 LOPD que refiere lo siguiente: no será preciso el consentimiento cuando los datos de carácter personal se recojan para el ejercicio de las funciones propias de las Administraciones Públicas en el ámbito de sus competencias; cuando se refieran a las partes de un contrato o precontrato de una relación negocial, laboral o administrativa y sean necesarios para su mantenimiento o cumplimiento; cuando el tratamiento de los datos tenga por finalidad proteger un interés vital del interesado en los términos del artículo 7 apartado 6 de la presente Ley, o cuando los datos figuren en fuentes accesibles al público y su tratamiento sea necesario para la satisfacción del interés legítimo perseguido por el responsable del fichero o por el del tercero a quien se comuniquen los datos, siempre que no se vulneren los derechos y libertades fundamentales del interesado. De no existir tal inequívoco consentimiento el tratamiento de datos que tal operación comporta podrá ser calificado como infracción muy grave de cesión in consentida de datos. Así lo ha entendido las

3.6.2 Derecho de consulta

El art. 14 LOPD, regula el derecho de Consulta al Registro General de Protección de Datos, y menciona que cualquier persona podrá conocer, recabando a tal fin la información oportuna de dicho Registro, la existencia de tratamientos de datos de carácter personal, sus finalidades y la identidad del responsable del tratamiento. El Registro General será de consulta pública y gratuita. Cuando dicho artículo cita “cualquier persona”, lo hace refiriéndose a la legitimidad para solicitar la información en dicho Registro, por lo que, corresponde a todo ciudadano, y puede recabarla no sólo el afectado o interesado en obtener la identificación del responsable del tratamiento, sino también los responsables del fichero a fin de comprobar los datos de los mismos incluidos en tal Registro (Lesmes Serrano *et al.*, 2008: 340).

El RD 1332/1994, de 20 de junio, en su art. 6 sobre notificación de ficheros de titularidad privada, refiere que la persona o entidad que pretenda crear un fichero de datos de carácter personal lo notificará previamente a la Agencia de Protección de Datos mediante escrito o soporte informático en el que se especificará lo siguiente: a) Nombre, denominación o razón social, documento nacional de identidad o código de identificación fiscal, dirección y actividad u objeto social del responsable del fichero; b) Ubicación del fichero; c) Identificación de los datos que se pretendan tratar, individualizando los supuestos de datos especialmente protegidos; d) dirección de la oficina o dependencia en la cual puedan ejercerse los derechos de acceso, rectificación y cancelación; e) Origen o procedencia de los datos; f) finalidad del fichero; g) Cesiones de datos previstas; h) Transferencias temporales o definitivas que se prevean realizar a otros países, con expresión de los mismos; i) Destinatarios o usuarios previstos para las cesiones o transferencias; j) Sistemas de tratamiento automatizado que se vayan a utilizar; y k) Medidas de seguridad.

El derecho de consulta, es posible gracias a la publicidad de los registros contemplada y ordenada por la Ley Orgánica de la materia. Entre las funciones

SSAN, Sección 1ª, de 18 de enero e 2002 (rec. 924/2000), 14 de junio de 2002 (rec. 650/2001) y 15 de noviembre de 2002 (rec. 732/2002) (Lesmes Serrano *et al.*, 2008: 337-338).

encomendadas a la Agencia de Protección de Datos en el art. 37.1 j) LOPD, se encuentra la de velar por la publicidad de la existencia de los ficheros de datos de carácter personal, para lo cual se publicará periódicamente una relación de dichos ficheros con la información adicional que el Director de la Agencia determine. El art. 39.2.e) LOPD, contempla el Registro General de Protección de Datos, como órgano integrado en la Agencia de Protección de Datos y al que corresponde facilitar al ciudadano el ejercicio de los derechos de información, accesos, rectificación, cancelación y oposición.

El principio de publicidad de los datos se vincula directamente con el derecho de los ciudadanos a conocer la totalidad de los tratamientos de carácter personal, tal derecho quedará satisfecho, con las mayores garantías si, conforme al art. 14 LOPD, su publicidad procede de una única fuente que, inmediatamente, incorpora cuantos tratamientos son objeto de notificación, pues dicha notificación es requisito necesario y previo a la existencia misma de la actividad de tratamiento (Lesmes Serrano *et al.*, 2008: 340).

3.6.3 Derecho de acceso

El art. 15 LOPD, regula el derecho de acceso, y en sus tres apartados precisa que: 1) El interesado tendrá derecho a solicitar y obtener gratuitamente información de sus datos de carácter personal sometidos a tratamiento, el origen de dichos datos así como las comunicaciones realizadas o que se prevén hacer de los mismos; 2) La información podrá obtenerse mediante la mera consulta de los datos por medio de su visualización, o la indicación de los datos que son objeto de tratamiento mediante escrito, copia, telecopia o fotocopia, certificada o no, en forma legible e inteligible, sin utilizar claves o códigos que requieran el uso de dispositivos mecánicos específicos; y 3) El derecho de acceso a que se refiere este artículo sólo podrá ser ejercitado a intervalos no inferiores a doce meses, salvo que el interesado acredite un interés legítimo al efecto, en cuyo caso podrá ejercitarlo antes.

Es el derecho del afectado a obtener información sobre sus propios datos de carácter personal y si están siendo objeto de tratamiento, la finalidad del tratamiento que, en su caso, se esté realizando, así como la información

disponible sobre el origen de dichos datos y las comunicaciones realizadas o previstas de los mismos. En virtud de este derecho, el afectado podrá obtener del responsable del tratamiento información relativa a datos concretos, incluidos en un determinado fichero, o a la totalidad de sus datos sometidos a tratamiento¹⁷⁵.

El derecho de acceso a los ficheros automatizados, así como los de rectificación y cancelación de datos deberán realizarse por el titular de los mismos, es decir, serán ejercidos por el afectado frente al responsable del fichero, sin otras limitaciones que las previstas por la ley de la materia. Podrá actuar el representante legal del afectado, en caso de incapacidad o minoría de edad¹⁷⁶.

La denegación del acceso se efectuará por el responsable del fichero cuando el derecho ya se haya ejercitado en los doce meses anteriores a la solicitud, salvo que acredite un interés legítimo al efecto. También podrá denegarse el acceso en los supuestos que así prevea una Ley o una norma de derecho comunitario de aplicación directa¹⁷⁷.

La SAN 29/2006, refiere que el habeas data (habeas scriptum), es el derecho que consiste en que el afectado puede exigir al responsable del fichero una prestación de hacer, consistente en la mera exhibición de sus datos y, en su caso, su rectificación o cancelación. Este derecho se encuentra en el art. 8.b) y c) del Convenio 108 del Consejo de Europa, así como en los arts. 12 y 14 de la

¹⁷⁵ Art. 27.1 RD 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de Desarrollo de la LO 15/1999, de 13 de diciembre, de protección de datos de carácter personal. Asimismo, el art. 28.1 RD 1720/2007, refiere que al ejercitar el derecho de acceso, el afectado podrá optar por recibir la información a través de uno o varios de los siguientes sistemas de consulta del fichero: a) visualización en pantalla; b) escrito, copia o fotocopia remitida por correo, certificado o no; c) telecopia; d) correo electrónico u otros sistemas de comunicaciones electrónicas; y e) cualquier otro sistema que sea adecuado a la configuración o implantación material del fichero o a la naturaleza del tratamiento, ofrecido por el responsable. Véase Agencia de Protección de Datos de la Comunidad de Madrid, 2008: 597-599.

¹⁷⁶ Art. 11 RD 1332/1994, lo referido en este dispositivo es con las limitaciones previstas por el propio Real Decreto y la LOPD. Los ficheros automatizados son los que guardan los datos personales en soportes informatizados, a los que se accede, a su vez, mediante programas o sistemas informáticos. Es la facilidad y la potencia de acceso que permite la tecnología informática la que ha dado lugar a la actual legislación de protección de datos personales, que no era necesaria cuando el acceso a esos datos se efectuaba manualmente (Agencia de Protección de Datos de la Comunidad de Madrid, 2009: 56).

¹⁷⁷ Art. 30 RD 1720/2007, en todo caso, el responsable del fichero informará al afectado de su derecho a recabar la tutela de la Agencia Española de Protección de Datos o, en su caso, de las autoridades de control de las comunidades autónomas, conforme a lo dispuesto en el art. 18 LOPD.

Directiva 95/46/CE. Por lo tanto, es indiscutible que el derecho de acceso constituye el núcleo esencial del derecho regulado en el art. 18.4 CE, porque sólo después de ejercitar este derecho, es que se puede proceder a la rectificación o cancelación.

Esta Sentencia de la Audiencia Nacional hace alusión al hecho de que el responsable del fichero utiliza datos del afectado en su beneficio, por tanto, le hace asumir una serie de cargas en garantía de los derechos del afectado, una de estas es el derecho de acceso. Carga que el responsable del fichero debe asumir con una especial diligencia dada la sensibilidad de los bienes jurídicos objeto de protección en el tráfico en el que opera. Cuando no se atiende el derecho de acceso se puede acudir al procedimiento de tutela previsto en la Ley. Dicho procedimiento de tutela no es un procedimiento sancionador¹⁷⁸.

Como se ha destacado antes, los derechos están íntimamente ligados con contenidos de otras disposiciones. La mayoría de las ocasiones, la persona podrá ejercitar este derecho de acceso, siempre y cuando esté enterada de qué sujeto responsable tiene a su cargo el manejo de su información personal, y esto es posible a través del derecho a la información previa, contenido en el art. 5 LOPD, que se da al momento de la recogida de los datos¹⁷⁹.

El titular de los datos tiene asimismo derecho a solicitar y obtener información sobre las comunicaciones realizadas o que se vayan a realizar, respecto de sus datos tratados. Comunicaciones que hacen referencia a las “cesiones” de datos personales, tal y como se definen en el apartado 1) del artículo 3 de la LOPD y se regulan en el artículo 11 de la LOPD (Lesmes Serrano, 2008: 346).

3.6.4 Derecho de rectificación y cancelación

El art. 16 LOPD, regula lo concerniente al derecho de rectificación y cancelación. Establece que: 1) El responsable del tratamiento tendrá la obligación de hacer efectivo el derecho de rectificación o cancelación del interesado en el

¹⁷⁸ SAN 29/2006, de 9 de Febrero, fundamento de derecho 3.

¹⁷⁹ Derecho a la información previa que se hace en la recogida de datos y que curiosamente esta dentro del apartado de “principios” en la LOPD.

plazo de diez días; 2) Serán rectificadas o canceladas, en su caso, los datos de carácter personal cuyo tratamiento no se ajuste a lo dispuesto en la LOPD y, en particular, cuando tales datos resulten inexactos o incompletos; 3) La cancelación dará lugar al bloqueo de los datos, conservándose únicamente a disposición de las Administraciones Públicas, Jueces y Tribunales, para la atención de las posibles responsabilidades nacidas del tratamiento, durante el plazo de prescripción de éstas. Cumplido el citado plazo deberá procederse a la supresión; y 4) Si los datos rectificadas o canceladas hubieran sido comunicados previamente, el responsable del tratamiento deberá notificar la rectificación o cancelación efectuada a quien se hayan comunicado, en el caso de que se mantenga el tratamiento por este último, que deberá también proceder a la cancelación¹⁸⁰.

Los derechos de rectificación o cancelación guardan estrecha relación con el principio de calidad del dato (art. 4.3 LOPD). De hecho, muchas de las sanciones por infracción del principio de exactitud y veracidad de los datos, que se revisan en vía contencioso-administrativa, derivan de un previo ejercicio, por el interesado, de los derechos de rectificación y, sobre todo, de cancelación, a los que el responsable del fichero no ha dado cumplimiento, o no de modo adecuado (Lesmes Serrano, 2008: 361)¹⁸¹.

Para mayor abundamiento de este tema y para explicarlo con un caso práctico y particular, es interesante la SAN de 16 de enero de 2008, que considera

¹⁸⁰ Art. 32 RD 1720/2007, regula el ejercicio de los derechos de rectificación y cancelación. Establece que: 1) La solicitud de rectificación deberá indicar a qué datos se refiere y la corrección que haya de realizarse y deberá ir acompañada de la documentación justificativa de lo solicitado. En la solicitud de cancelación, el interesado deberá indicar a qué datos se refiere, aportando al efecto la documentación que lo justifique, en su caso; 2) El responsable del fichero resolverá sobre la solicitud de rectificación o cancelación el plazo máximo de diez días a contar desde la recepción de la solicitud. Transcurrido el plazo sin que de forma expresa se responda a la petición, el interesado podrá interponer la reclamación prevista en el art. 18 LOPD. En el caso de que no disponga de datos de carácter personal del afectado deberá igualmente comunicárselo en el mismo plazo; y 3) Si los datos rectificadas o canceladas hubieran sido cedidos previamente, el responsable del fichero deberá comunicar la rectificación o cancelación efectuada al cesionario, en idéntico plazo, para que éste, también en el plazo de diez días contados desde la recepción de dicha comunicación, proceda, asimismo, a rectificar o cancelar los datos. La rectificación o cancelación efectuada por el cesionario no requerirá comunicación alguna al interesado.

¹⁸¹ La SAN, Sección 1ª, de 14 de septiembre de 2001 (rec. 368/2000) confirma la sanción por infracción grave el art. 43.3 f) LORTAD (artículo que coincide con el mismo numeral de la LOPD) respecto de la empresa que, a pesar de haber emitido certificación de la cancelación efectiva de los datos del denunciante, solicitada por él, con posterioridad le envió, a su nombre y domicilio, nueva correspondencia con publicidad (Lesmes Serrano, 2008: 361).

que los ficheros de los libros de bautismo están sujetos a la legislación en materia de protección de datos¹⁸². Los hechos se desarrollan en torno a una persona que solicita que sus datos sean cancelados en el libro de registros de bautismo en posesión de la iglesia, que no procede a realizar dicha solicitud, alegando que en ellos se anotan hechos históricos. Posteriormente, la interesada acude a la Agencia de Protección de Datos, que estima la reclamación y ordena la anotación marginal de cancelación de la inscripción en el correspondiente libro bautismal, así como la remisión de un certificado en el que se hiciera constar que la interesada había ejercido su derecho de cancelación.

La resolución de la Agencia Española de Protección de Datos, idéntica a otras muchas dictadas en procedimientos similares, fundamenta su decisión en el art. 4.3 LOPD, conforme al cual “los datos de carácter personal serán exactos y puestos al día de forma que respondan con veracidad a la situación actual del afectado”, principio que en este caso, entiende que debe verificarse mediante anotación marginal en la partida de bautismo del reclamante, a fin de que se haga constar el ejercicio de cancelación, hecho que no fue llevado a cabo por el Arzobispado.

Contra dicha resolución, el Arzobispado interpuso recurso contencioso-administrativo utilizando dos argumentos principales: en el primero, sostiene la inviolabilidad absoluta de los libros y registros de la iglesia católica frente a la acción del Estado, invocando el Convenio firmado con la Santa Sede¹⁸³; y en el

¹⁸² No sólo se plantea la colisión del derecho a la protección de datos personales con el derecho fundamental a la libertad de expresión. Se trata de un pleito promovido por el Arzobispado de Valencia contra las resoluciones de la Agencia Española de Protección de Datos que, atendiendo a aquellas personas que habían solicitado la cancelación de sus datos personales en los Libros de Bautismo, ordenaba al correspondiente Arzobispado que procediera a realizar una anotación marginal en dicho Libro de Bautismo haciendo constar que el afectado había ejercido su derecho de cancelación. En este pleito, entre otras cuestiones, se suscitaba la posible colisión entre el derecho de la Iglesia Católica a la libertad religiosa y el derecho fundamental también a la protección de datos que conlleva entre otras facultades el derecho a obtener la cancelación de los datos personales.

¹⁸³ Tal inviolabilidad se sustenta en el art. 1.6 del Acuerdo sobre Asuntos Jurídicos suscrito el 3 de enero de 1979 por la Santa Sede y el Estado Español, y en su derecho como iglesia o confesión religiosa a decidir libremente su organización y funcionamiento frente a cualquier intromisión del Estado, derecho fundamental consagrado en el art. 16.1 CE y en el art. 6 LO 7/1980, de libertad religiosa. Así la orden emitida por la Agencia Española de Protección de Datos instándole a realizar una determinada anotación en el libro registro de bautismo y emitir una certificación de constancia supondría una intromisión ilegítima por prohibida no sólo por una norma con rango de

segundo, considera incorrecta la aplicación de la LOPD, por sostener que los libros de bautismo no tienen la consideración de ficheros de datos en el sentido expresado por la citada Ley, no siendo por tanto de aplicación dicha norma, porque se registran hechos que verdaderamente sucedieron¹⁸⁴.

La SAN razona que conforme a la Ley de la materia, el nombre y apellido de una persona, registrados en un soporte físico (en este caso, papel), el cual permite su tratamiento, hace posible que estamos ante datos susceptibles de tratamiento. Recuerda que lo relevante para estar ante un tratamiento de datos personales es la realización de determinadas actuaciones en relación a los mismos, actuación que en su descripción son muy amplias y variadas. Así, los libros de bautismo, en la medida en que recogen datos de carácter personal (al menos el nombre y apellidos del bautizado y el hecho mismo de su bautismo) con arreglo a criterios preestablecidos que permiten su tratamiento, tienen la consideración de fichero y están sujetos, en cuanto tales, a la legislación en materia de protección de datos¹⁸⁵.

La Audiencia Nacional desestima el recurso por considerar que los libros de bautismo sí constituyen un fichero de personas que han recibido el sacramento del bautismo y en las que concurre únicamente una apariencia de pertenencia a la Iglesia. Por ello, no puede negarse que, por ejemplo, la expedición de una partida de bautismo sea una forma de tratamiento de datos personales y que estos, al estar contenidos en el libro de bautismo con arreglo a criterios preestablecidos, determinen que éste tenga la consideración legal de fichero.

ley como sería el Acuerdo referido sino también por la Constitución misma (SAN de 16 de enero de 2008, Fundamento de Derecho tercero).

¹⁸⁴ Añade que para el caso de que dicha norma sea aplicable, los datos recogidos en el libro de bautismo no son inexactos ni tienen porqué ser puestos al día, pues se limitan a constatar un hecho realmente ocurrido, hecho que no implica la pertenencia actual a la Iglesia Católica (SAN de 16 de enero de 2008, Fundamento de Derecho tercero).

¹⁸⁵ La SAN dice que, en este sentido, la contradicción que aprecia la parte recurrente en relación con la resolución impugnada es más aparente que real, pues si bien es cierto que la Agencia demandada señala que los “Libros de Bautismo (...) no pueden considerarse como un fichero de miembros de la Iglesia”, a pesar de ello sí considera que constituyen una “base de datos de carácter personal que conforme al artículo 2.2 (...) no se encuentra excluida del régimen de protección de la citada Ley Orgánica”. De manera que aunque los Libros de Bautismo no sean estrictamente un fichero de miembros de la Iglesia Católica, sí constituyen un fichero de personas que han recibido el sacramento del bautismo y en las que concurre únicamente una apariencia de pertenencia a la Iglesia sobre lo que luego insistiremos, pero basta ahora con señalar que esta circunstancia satisface las exigencias del artículo 2.2. de la Ley Orgánica 15/1999 (SAN de 16 de enero de 2008, Fundamento de Derecho cuarto).

Continuando con el análisis de esta Sentencia, particularmente interesante, el segundo punto de discrepancia del Arzobispado se refiere a la interpretación que la Agencia de Protección de Datos hace del principio de calidad de los datos, específicamente a la exactitud y veracidad de los mismos. La Administración entiende, con fundamento en el art. 4.3 LOPD, que determinados datos personales contenidos en los libros de bautismo no son exactos o, al menos, no están puestos al día de forma que respondan con veracidad a la situación actual del afectado.

En este sentido, el derecho fundamental a la protección de los datos del art. 18.4 CE encuentra en el principio del consentimiento un eslabón esencial, que otorga a la persona la posibilidad de determinar el nivel de salvaguardia de sus datos personales, cuya protección, por cierto, se encuentra reforzada en relación con los datos sensibles como sucede en este caso, con los relativos a las creencias religiosas. Derecho fundamental que extiende su protección no a los datos íntimos de la persona -que se protegen en el derecho a la intimidad-, sino a los datos de carácter personal (STC 292/2000), por lo que la garantía de la vida privada de la persona y su reputación poseen una dimensión positiva que excede del ámbito del art. 18.1 CE y que se traduce en un derecho al control sobre los datos por el titular de los mismos¹⁸⁶.

Por lo anterior, la Sentencia reflexiona que desde la perspectiva estricta del derecho fundamental a la protección de datos personales o autodeterminación informativa, el principio de calidad del dato se puede infringir si el responsable del fichero -en este caso el Arzobispado de Valencia- permanece impassible ante una petición de puesta al día de la información contenida en el Registro¹⁸⁷.

¹⁸⁶ Con el objeto de preservar este derecho fundamental, la LOPD establece una serie de principios generales en su Título II, que definen las pautas a las que debe atenerse la recogida, uso y desenvolvimiento de datos de carácter personal. Pautas o principios encaminados a garantizar tanto la veracidad de la información contenida en dichos datos, cuanto la congruencia y calidad de los mismos para salvaguardar el respeto al derecho fundamental a la protección de los datos personales. Y entre los cuales se recoge, en tal artículo 4.3 de la Ley, el de veracidad o exactitud de los datos, que trata de preservar y proteger la calidad y certeza de la información sometida a tratamiento, principio que la Agencia Española de Protección de Datos trata de garantizar por medio de su resolución (SAN de 16 de enero de 2008, Fundamento de Derecho quinto).

¹⁸⁷ El Fundamento de Derecho sexto de esta Sentencia, hace una reflexión importante sobre lo que el recurrente aprecia como una intrusión ilegítima del Estado a la iglesia, cuando lo que en realidad sucede es el ejercicio directo, por una persona, de un derecho fundamental. Este

Recientemente el Tribunal Constitucional ha inadmitido a trámite un recurso de amparo, promovido por al AEPD, al respecto de un contencioso que venía manteniendo desde hace un tiempo con el Arzobispado de Valencia¹⁸⁸. El recurso de amparo lo promovió luego que el Tribunal Supremo estimara el recurso de casación por Sentencia de 19 de septiembre de 2008, al considerar que los libros bautismales carecen del carácter de ficheros de datos en el sentido de la LOPD¹⁸⁹. Toda vez que esos datos personales estén recogidos en los libros de

Fundamento de Derecho, refiere que también la entidad recurrente, como motivo de impugnación en su recurso, al socaire del derecho a la libertad religiosa del artículo 16.1 de la CE y del Acuerdo entre el Estado Español y la Santa Sede, sobre Asuntos Jurídicos, de 3 de enero de 1979, que sus archivos resultan inviolables, en lo que hace al caso, y que, además, se podrían suprimir datos, como es el nombre y apellidos, pero no un hecho, como es el haber administrado el sacramento del bautismo. En relación con la aplicación del citado Acuerdo, la Sentencia señala que efectivamente se esta ante un Tratado Internacional, cuyo texto ha sido aprobado por las Cortes Generales y publicado oficialmente, lo que significa, en virtud de lo dispuesto en el art. 96 CE, que forma parte del ordenamiento jurídico español, en un lugar subordinado a la Constitución, atendida su posición en el sistema interno de fuentes del Derecho y atendidos los efectos previstos en los arts. 94 y 95 CE. Sentada esta posición del Tratado, en el sistema de jerarquía normativa, la regulación contenida en el mismo ha de ser interpretada conforme a la Constitución, concretamente conforme al derecho fundamental a la protección de los datos. A juicio la Sala de la Audiencia Nacional que resolvió la Sentencia, sin embargo, el citado Acuerdo no contradice la regulación constitucional y legalmente establecida del derecho fundamental a la protección de los datos, cuando en el artículo I apartado 6 dispone que “el Estado respeta y protege la inviolabilidad de los archivos, registros y demás documentos pertenecientes a la Conferencia Episcopal Española, a las Curias episcopales, a las Curias de los superiores mayores de las Órdenes y Congregaciones religiosas, a las parroquias y a otras instituciones y entidades eclesásticas”. Los archivos y registros relacionados en el citado artículo del Acuerdo Internacional se encuentran protegidos de cualquier intromisión procedente del Estado y resultan inviolables frente al mismo. Ahora bien, tal inviolabilidad no es predicable frente al ciudadano cuando ejercita el derecho fundamental previsto en el art. 18.4 CE, en cuyo contenido esencial se integra el poder de disposición sobre los datos relativos a su persona. La solución inversa a la expuesta, que postula el Arzobispado recurrente, equivaldría a reconocer una superioridad de la norma contenida en un Tratado, frente a la norma constitucional (SAN de 16 de enero de 2008, Fundamento de Derecho sexto).

¹⁸⁸ El auto por el que inadmite el recurso de amparo es el ATC 20/2011, de 28 de febrero de 2011. El 23 de mayo de 2006, la AEPD estimó la tutela de derechos (TD/00046/2006), por la que se ordenaba al Arzobispado de Valencia anotar en el libro de bautismo la solicitud de cancelación realizada por una persona. El 10 de octubre de 2007, la Audiencia Nacional desestima el recurso interpuesto por el Arzobispado contra la resolución de la AEPD. El 19 de septiembre de 2008, el Tribunal Supremo estimó el recurso de casación interpuesto por el Arzobispado contra la Sentencia de la Audiencia Nacional, en consecuencia esta Sentencia del Tribunal Supremo anula la Resolución inicial de la AEPD. El 12 de noviembre de 2008, el TS inadmitió el incidente de nulidad de actuaciones promovido por la AEPD. El auto en cuestión inadmite el recurso de amparo presentado por la AEPD contra esta providencia. El TC considera que la Agencia adolece de falta de legitimación activa para interponer el recurso, puesto que no es titular (en este caso) del derecho a la tutela judicial efectiva, ni (en ningún caso) del derecho a la protección de datos personales. El TC estima que sólo los titulares de los derechos, el Defensor del Pueblo y el Ministerio Fiscal estarían legitimados.

¹⁸⁹ La Sentencia de 19 de septiembre de 2008, de la Sala III de lo Contencioso-Administrativo del Tribunal Supremo, contiene un interesante voto particular formulado por el Magistrado Joaquín Martínez de Velasco, en el que refiere que “Quinto.- (...) la Directiva define los ficheros como «todo conjunto estructurado de datos personales, accesibles con arreglo a criterios determinados».

bautismo, como un conjunto organizado tal y como exige el art. 3.b) LOPD, sino

El bautismo debe ser inscrito, sin demora, por el párroco con indicación del nombre del bautizado, haciendo mención del sacerdote que lo administró, de los padres, los padrinos y los testigos, si los hubo, indicando el día de la celebración, así como la fecha y el lugar del nacimiento del bautizando (canon 877, § 1, del Código de Derecho Canónico, de 25 de enero de 1983). En el libro de bautizados se anota también la confirmación así como el estado canónico de los fieles por razón de matrimonio, anotaciones que han de hacerse constar en la partida de bautismo (canon 535). Habida cuenta del fundamento de la decisión mayoritaria, de la noción comunitaria de fichero de datos personales y de la ordenación canónica de la inscripción bautismal, me pregunto si los libros que contienen los bautismos administrados, con indicación del día, del nombre y apellidos del neófito, así como del lugar y de la fecha de su nacimiento dejan de ser ficheros por la circunstancia de que no estén ordenados alfabéticamente ni por esa última fecha. O, dicho de otra manera, dudo que la ordenación con arreglo a la jornada en que se celebró el sacramento no sea un «criterio determinado» de acceso, impidiendo tildar a estos libros parroquiales de «conjunto estructurado de datos». Reconozco que la búsqueda resulta más fácil cuanto mayor sea el número de parámetros disponibles, pero no sé qué grado de dificultad en el examen determina que un conjunto estructurado de datos personales deje de considerarse un fichero a los efectos de someterlo a la legislación comunitaria armonizada. ¿Dónde se fija el umbral? Creo que existen dudas razonables sobre el alcance de las nociones de derecho comunitario que se manejan en la Sentencia. Tengo la convicción de que los magistrados que defienden la opinión mayoritaria, que no comparten mis dudas, no están, sin embargo, seguros de que los jueces de otros Estados miembros y el Tribunal de Justicia participen de su criterio. Si a lo anterior se añade que la interpretación de dichas nociones tiene directa incidencia en el desenlace de este recurso, pues, según sea la extensión que se les otorgue, los libros parroquiales de bautismo tendrán la consideración de ficheros de datos personales, quedando sometidos a la normativa sectorial, con las consecuencias inherentes, estimo que la Sala, antes de decidir, debió, tras oír a las partes y al Ministerio Fiscal, remitirse al Tribunal de Justicia a título prejudicial para preguntarle si, a los efectos del repetido concepto de fichero, que contiene la Directiva: 1º) Las indicaciones personales como las que aparecen en los libros de bautismo constituyen un conjunto estructurado de datos de esa naturaleza; 2º) La ordenación de un registro con arreglo a la fecha en la que sea realizan los actos inscritos constituye un criterio determinado de accesibilidad; 3º) Ese modo de estructurar un archivo dificulta de tal manera la búsqueda que impide calificarlo de «fichero de datos personales». Si la interpretación facilitada por el Tribunal de Justicia condujera a considerar ficheros los libros bautismales, habría que preguntarse por la noción de «tratamiento de datos personales» del artículo 2, letra b), de la Directiva, reproducida, con otras palabras, en el artículo 3, letra c), de la Ley Orgánica 15/1999. No queda claro de su redacción si el tratamiento se produce con el mero archivo, registro, conservación o requiere, además, su extracción, cesión, difusión o transferencia y, en este último caso, qué incidencia tiene para dar contenido al concepto que esos datos únicamente puedan extraerse mediando petición del interesado, satisfecha a través de la emisión de una partida o certificación. Dicho de otra forma, resulta indispensable saber si la noción de «tratamiento» requiere que los datos sean efectivamente manejados, cotejados o interconectados, o basta la mera posibilidad de su uso con tal alcance, puesto que, aunque las partidas de bautismo sólo se emiten a instancia de la persona directamente concernida, la práctica cotidiana nos enseña que la consulta de los libros parroquiales por terceros (investigadores, estudiosos o personas con otros intereses legítimos) no es una situación extravagante. A mi entender, las consideraciones que preceden alcanzan mayor calado y se cargan de razón si se toma en consideración que el presente recurso de casación se refiere a unos datos que, como las convicciones religiosas, tocan el núcleo de un derecho fundamental (artículo 16, apartado 2, de la Constitución), que la Directiva (artículo 8), como la Ley Orgánica 15/1999 (artículo 7), considera especialmente protegidos. Sexto.- En suma, esta Sala conoce en última instancia un litigio en el que para decidir ha manejado conceptos autónomos de derecho comunitario, incluidos en una Directiva que persigue la armonización completa de las normativas nacionales sobre protección de datos personales, cuya interpretación no se impone de modo indubitado, por lo que, en virtud de los anteriores argumentos y con arreglo al artículo 234 del Tratado constitutivo de la Comunidad Europea, debió dirigirse al Tribunal de Justicia para, a título prejudicial, interrogarle en los términos expresados”.

que resultan ser una pura acumulación de estos que comporta una difícil búsqueda, acceso e identificación en cuanto no están ordenados ni alfabéticamente, ni por fecha de nacimiento, sino sólo por las fechas de bautismo, siendo absolutamente necesario el conocimiento previo de la parroquia donde aquel tuvo lugar, no resultando además accesibles para terceros distintos del bautizado, que no podrían solicitar ajenas partidas de bautismo. Además la Sentencia dice que el art. 4.3 LOPD señala que los datos de carácter personal serán exactos y puestos al día de forma que respondan con veracidad a la situación actual del afectado. Pues bien, en los libros de bautismo no cabe apreciar ninguna inexactitud de datos, en cuanto en los mismos se recoge un dato histórico cierto, salvo que se acredite la falsedad, cual es el referente al bautismo de una persona y cuando esta solicita la cancelación de ese hecho, no está pretendiendo que se corrija una inexactitud en cuanto al mismo, sino que en definitiva está intentando y solicitando un sistema nuevo y diferente de registro de nuevos datos personales.

3.6.5 Derecho de oposición

El derecho de oposición consiste en la facultad que tiene el interesado, en determinada circunstancia, de oponerse al tratamiento de los datos que le conciernen, en cuyo caso, previa petición y de forma gratuita, serán dados de baja del tratamiento, cancelándose la información que sobre ellos figuren en un determinado registro, a su simple solicitud¹⁹⁰. Es decir, el derecho de oposición consiste en la negativa por parte del interesado a la continuación del tratamiento de sus datos personales (Díaz-Arias, 2008: 71).

Se trata de uno de los derechos de las personas introducido escuetamente, y por primera vez, en la LO 15/1999¹⁹¹. La anterior LORTAD no lo preveía (Lesmes Serrano *et al*, 2008: 379). El art. 6.4 LOPD prevé que en los casos en los que no sea necesario el consentimiento del afectado para el tratamiento de los datos de carácter personal, y siempre que una Ley no disponga lo contrario, éste

¹⁹⁰ El art. 30.4 LOPD (tratamiento con fines de publicidad y de prospección comercial), refiere que los interesados tendrán derecho a oponerse, previa petición y sin gastos, al tratamiento de los datos que les conciernan, en cuyo caso serán dados de baja del tratamiento, cancelándose las informaciones que sobre ellos figuren en aquél a su simple solicitud.

¹⁹¹ En atención al art. 14 de la Directiva 46/95/CE.

podrá oponerse a su tratamiento cuando existan motivos fundados y legítimos relativos a una concreta situación personal. En tal supuesto, el responsable del fichero excluirá del tratamiento los datos relativos al afectado¹⁹².

En la LOPD el derecho de oposición aparece limitado en su nacimiento y condicionado en su ejercicio, pues sólo se aplicaría en los casos en que no sea necesario el consentimiento del interesado. Ello en definitiva parece lógico pues en el caso contrario debería bastarle al afectado con negarse a prestar su consentimiento, o revocarlo en el momento que así lo deseara, para que dicho tratamiento no se produjera. Sin embargo debe tenerse en cuenta que la revocación también está sujeta a unas condiciones legales como son que exista causa justificada para ello y que no se le atribuyan efectos retroactivos (Corripio Gil-Delgado, 2000: 227-228). Por su parte, Guerrero Picó (2006: 304-305) recuerda que este derecho es calificado como una de las “innovaciones más enigmáticas”, y que a falta de desarrollo reglamentario, la incertidumbre ha persistido en la doctrina durante mucho tiempo, además de que lo asimila al derecho de revocación del consentimiento, cuando éste precisamente, no se requiere.

En cuanto a los datos incluidos en las fuentes de acceso público, la Ley de la materia determina que el afectado puede solicitar que se *excluya* la utilización de sus datos obrantes en los Colegios Profesionales, con fines de publicidad o prospección comercial. Asimismo, se establece que los interesados tendrán derecho a *oponerse*, previa petición y sin gastos, al tratamiento de los datos que les conciernan, en cuyo caso serán dados de baja, cancelándose la información que sobre ellos figure en dicho tratamiento, a su simple solicitud¹⁹³.

¹⁹² Los arts. 17 y 18.2 LOPD hacen referencia al procedimiento que deberá ser establecido reglamentariamente, sin contraprestación alguna y de la tutela de derechos.

¹⁹³ Arts. 28.2 y 30.4 LOPD. Las Reglas Heredia de 2003 para América Latina, tienen el objetivo de servir como modelo a ser adoptado por los tribunales e instituciones responsables de la divulgación de jurisprudencia de todos los países de América Latina. La finalidad de estas es la difusión en Internet de las sentencias y resoluciones judiciales, siendo el conocimiento de la información jurisprudencial y la garantía de igualdad ante la ley, y para procurar alcanzar la transparencia de la administración de justicia. La Regla 3 dice que se reconocerá al interesado el derecho a oponerse, previa petición y sin gastos, en cualquier momento y por razones legítimas propias de su situación particular, a que los datos que el conciernan sean objeto de difusión, salvo cuando la legislación nacional disponga otra cosa. En caso de determinarse, de oficio o a petición

El derecho de oposición es el derecho del afectado a que no se lleve a cabo el tratamiento de sus datos de carácter personal o se cese el mismo en los siguientes supuestos: a) cuando no sea necesario su consentimiento para el tratamiento, como consecuencia de la concurrencia de un motivo legítimo y fundado, referido a su concreta situación personal, que lo justifique, siempre que una Ley no disponga lo contrario; b) cuando se trate de ficheros que tengan por finalidad la realización de actividades de publicidad y prospección comercial, cualquiera que sea responsable de su creación; y c) cuando el tratamiento tenga por finalidad la adopción de una decisión referida al afectado y basada únicamente en un tratamiento automatizado de sus datos de carácter personal (art. 34 RD 1720/2007).

En lo que hace al ejercicio del derecho de oposición, el responsable del fichero o tratamiento deberá excluir del mismo, los datos relativos al afectado que ejercite su derecho o denegar motivadamente la solicitud. Este derecho también se podrá ejercitar en decisiones basadas en un tratamiento automatizado de datos, es decir, los interesados 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 automatizado de datos destinado a evaluar determinados aspectos de su personalidad, tales como su rendimiento laboral, crédito, fiabilidad o conducta¹⁹⁴.

La STC 292/2000, recuerda que la llamada "libertad informática" es el derecho a controlar el uso de los datos insertos en un programa informático (*habeas data*) y comprende, entre otros aspectos, la oposición del ciudadano a que determinados datos personales sean utilizados para fines distintos de aquel legítimo que justificó su obtención. Además el derecho a consentir el conocimiento y el tratamiento, informático o no, de los datos personales, requiere como complementos indispensables, por un lado, la facultad de saber en todo momento quién dispone de esos datos personales y a qué uso los está sometiendo, y, por otro lado, el poder oponerse a esa posesión y usos. Y resultan

de parte, que datos de personas físicas o jurídicas están ilegítimamente siendo difundidos, deberá ser efectuada la exclusión o rectificación correspondiente.

¹⁹⁴ Arts. 35 y 36 RD 1720/2007.

indispensables para hacer efectivo el contenido del derecho a la protección de datos, el reconocimiento del derecho a ser informado de quién posee sus datos personales y con qué fin, y el derecho a poder oponerse a esa posesión y uso requiriendo a quien corresponda que ponga fin a la posesión y empleo de los datos. Es decir, exigiendo del titular del fichero que le informe de qué datos posee sobre su persona, accediendo a sus oportunos registros y asientos, y qué destino han tenido, lo que alcanza también a posibles cesionarios; y, en su caso, requerirle para que los rectifique o los cancele (SSTC 11/1998, FJ 5, 94/1998, FJ 4).

3.6.6 Derecho de indemnización

El art. 19 LOPD contempla el derecho a indemnización, y en sus tres apartados precisa lo siguiente: 1. Los interesados que, como consecuencia del incumplimiento de lo dispuesto en la presente Ley por el responsable o el encargado del tratamiento, sufran daño o lesión en sus bienes o derechos tendrán derecho a ser indemnizados; 2. Cuando se trate de ficheros de titularidad pública, la responsabilidad se exigirá de acuerdo con la legislación reguladora del régimen de responsabilidad de las Administraciones Públicas; y 3. En el caso de los ficheros de titularidad privada, la acción se ejercitará ante los órganos de la jurisdicción ordinaria.

La Sala de lo Contencioso-administrativo de la Audiencia Nacional tiene atribuido, a causa de la disposición adicional 4.5 de la Ley 28/1998, de 13 de julio, el conocimiento, en única instancia, de los actos administrativos dictados por la Agencia Española de Protección de Datos. Sin embargo ha sido doctrina reiterada y constante de tal Sala, que carece de competencia para pronunciarse, en dichos procedimientos frente a resoluciones de la AEPD, sobre la existencia o inexistencia de una eventual indemnización a favor de los interesados que hayan podido sufrir daño o lesión en sus bienes o derechos, por eventuales incumplimientos de dicha normativa sobre protección de datos (Lesmes Serrano *et al.*, 2008: 396)¹⁹⁵.

¹⁹⁵ La SAN, Sección 1ª, de 18 de mayo de 2001 (rec. 856/1999), respecto de la anterior LORTAD, dice que quizás convenga indicar que las indemnizaciones a que se refiere el art. 17.3 de la Ley

Tal y como ya declaró la Sala de la Audiencia Nacional, Sección 1ª, de 18 de mayo de 2001 (rec. 856/1999) respecto de la anterior LORTAD: “(...) quizás convenga indicar, como bien razona el Sr. Abogado del Estado, que las indemnizaciones a que se refiere el artículo 17.3 de la Ley (artículo 19.1 de la LOPD), no las declara la Agencia, sino que el afectado que sufra lesión o daño en sus bienes o derechos podrá reclamarla en la vía civil o administrativa”.

En cuanto a la indemnización respecto de ficheros de titularidad pública contenida en el art. 19.2 LOPD, conecta con la exigencia de responsabilidad con la legislación reguladora del régimen de responsabilidad de las Administraciones Públicas. Se trata de una concreción del principio general contenido en el art. 106.2 CE, que otorga a los particulares el derecho a ser indemnizados en toda lesión que sufran en sus bienes y derechos, en los términos establecidos en la Ley, y salvo de fuerza mayor, siempre que la lesión sea consecuencia el funcionamiento de los servicios públicos¹⁹⁶.

En lo que hace a los ficheros de titularidad privada, ya se ha dicho que se ejercita ante los órganos de jurisdicción ordinaria. Es interesante lo que anota Lesmes Serrano (2008: 397) al referir que en la LORTAD, el derecho de indemnización, podía dar lugar a inequívocos, pues al contenerse en el mismo precepto que el procedimiento de tutela de derechos, no estaba muy claro si era o no obligada la previa reclamación del afectado ante la AEPD, para poder ejercitar, con posterioridad, la acción indemnizatoria ante la jurisdicción ordinaria. Pero que, de la literalidad del actual art. 19 LOPD, sin embargo, no

(art. 19.1 LOPD), no las declara la Agencia, sino que el afectado que sufra lesión o daño en sus bienes o derechos podrá reclamarla en la vía civil o administrativa. La STS, Sala 3ª, de 28 de diciembre de 2004 (rec. 3020/2001) expone que la situación jurídica de los denunciantes-recurrentes no experimenta ventaja alguna por el hecho de que se sancione a la entidad bancaria denunciada, único pronunciamiento que cabría pretender de la AEPD, ya que la pretensión indemnizatoria articulada por los actores no puede ser atendida por la Agencia, sino que deberá, en su caso, ser instada ante los órganos del orden jurisdicción civil a través del cauce procesal pertinente, ni la prosperabilidad de dicha pretensión queda supeditada o condicionada a la imposición de una previa sanción a la denunciada. La SAN, Sección 1ª, de 8 de marzo de 2004 (rec. 424/2004) argumenta que por lo que se refiere a la indemnización solicitada en concepto de daños morales, el art. 19.3 LOPD establece que en los casos de los ficheros de titularidad privada, la acción se ejercitará ante los órganos de la jurisdicción ordinaria, siendo por tanto dichos órganos y no la AEPD, los competentes para pronunciarse sobre el particular (Lesmes Serrano *et al.*, 2008: 396).

¹⁹⁶ De exigirse la responsabilidad patrimonial del Estado por el funcionamiento de la Administración de Justicia, habrá de considerarse la regulación en los arts. 292 a 297 LO 6/1985.

parece desprenderse tal necesidad de previa reclamación ante la Agencia, para poder acudir a la jurisdicción civil, a fin de ejercitar la pretensión indemnizatoria prevista en el precepto para los ficheros de titularidad privada. Por lo que, se trata en definitiva, de órdenes jurisdiccionales distintos, en los que se ejercitan diferentes pretensiones: en vía contencioso administrativa por vulneración de alguno de los derechos contemplados en la normativa de protección de datos, y en cambio, en vía civil, por los daños y perjuicios derivados de una eventual lesión de dicha normativa de protección de datos, respecto de los ficheros privados¹⁹⁷.

3.6.7 Tutela de los derechos (reclamación y la tutela de los derechos)

A la Agencia Española de Protección de Datos se le encomiendan, entre otras, funciones de policía. Ha de vigilar de oficio la correcta actuación de los operadores en el sistema de protección de los datos de carácter personal, su adecuación a los principios que marca la LOPD; para ello están las inspecciones de oficio (Guerrero Picó, 2006: 310).

El art. 18 LOPD, dispone que las actuaciones contrarias a lo dispuesto en la Ley pueden ser objeto de reclamación por los interesados ante la AEPD, en la forma que reglamentariamente se determine. El interesado al que se deniegue, total o parcialmente, el ejercicio de los derechos de oposición, acceso, rectificación o cancelación, podrá ponerlo en conocimiento de la Agencia o, en su caso, del Organismo competente de cada Comunidad Autónoma, que deberá asegurarse de la procedencia o improcedencia de la denegación¹⁹⁸. Contra las resoluciones de la Agencia de Protección de Datos procederá recurso contencioso-administrativo.

¹⁹⁷ De hecho dicen los autores que han sido múltiples las reclamaciones de los interesados ante los órganos de la jurisdicción civil, por considerar incumplido alguno de sus derechos garantizados en la LOPD, por parte del responsable del tratamiento o del fichero, reclamaciones en las que han solicitado la correspondiente indemnización (especialmente en los supuestos de indebida inclusión de sus datos personales en los ficheros sobre solvencia patrimonial y crédito), dando lugar a numerosos pronunciamientos judiciales.

¹⁹⁸ Art. 18.3 LOPD refiere que el plazo máximo en que debe dictarse la resolución expresa de tutela de derechos será de seis meses. Ordinales 1 y 4 coinciden con los apartados 1 y 2 del artículo 17 de la LORTAD, y los que constituían los apartados 3, 4 y 5 de aquel artículo 17 de la LORTAD presentan gran similitud con el actual artículo 19 de la LOPD. Esta ley, a diferencia de la LORTAD, ha separado la tutela de los derechos del derecho a la indemnización.

Una de las características de este derecho es que la LOPD establece un sistema jurídica para la tutela de los derechos personales que gira sobre la actuación de la AEPD y se inicia por medio de una reclamación cuyo plazo inicial no está previsto ni en la norma legal ni en las reglamentarias y que, por tanto, hay que entender que no está sometido a otros plazos que el de la prescripción general de los derechos (Palomar Olmeda, 2007: 39).

El Procedimiento de tutela de derechos de acceso, rectificación, cancelación y oposición se encuentra regulado en el Capítulo II del RD 1720/2007. En él se prevé que el procedimiento se iniciara a instancia del afectado ante la Agencia Española de Protección de Datos, y que el plazo máximo para dictar la resolución será de seis meses.

3.7 Límites

Los derechos fundamentales no son ilimitados, cada uno tiene un objeto o contenido más o menos preciso, que otorga protección jurídica a un concreto ámbito de actuación, y presenta, por tanto, unas fronteras o contornos más o menos definidos. Los límites a los derechos fundamentales son normas que restringen su objeto de protección y por ello sólo podrán ser adoptados de conformidad con la Constitución. Estos límites suponen la adopción de normas que establecen obligaciones y prohibiciones en relación al objeto de protección del derecho fundamental (Villaseñor Goyzueta, 2011: 43-44).

El TCE en las Sentencias relativas al derecho de protección de datos ha declarado que este no es ilimitado, y aunque la Constitución no le imponga expresamente límites específicos, ni remita a los Poderes Públicos para su determinación como ha hecho con otros derechos fundamentales, no cabe duda de que han de encontrar dichos límites en el resto de derechos fundamentales y bienes jurídicos constitucionalmente protegidos, como lo exige el principio de unidad de la Constitución (STC 292/2000, FJ 11)¹⁹⁹.

Esos límites pueden ser restricciones directas del propio derecho fundamental o bien pueden ser restricciones al modo, tiempo o lugar de ejercicio

¹⁹⁹ SSTC 11/1981, FJ 7; 196/1987, FJ 6; y respecto del art. 18, la STC 110/1984, FJ 5.

del mismo. En el primer caso, regular esos límites es una forma de desarrollo del derecho fundamental. Mientras que en segundo, los límites que se fijan lo son a la forma concreta en la que cabe ejercer el haz de facultades que compone el contenido del derecho en cuestión, constituyendo una manera de regular su ejercicio²⁰⁰.

En este sentido, la primera constatación que debe hacerse -que no por evidente es menos capital- es que la Constitución ha querido que sólo la Ley pueda fijar los límites a los derechos fundamentales. Estos pueden ceder ante bienes e incluso intereses constitucionalmente relevantes, siempre que el recorte que experimenten sea necesario para lograr el fin legítimo previsto, proporcionado para alcanzarlo y sea respetuoso con el contenido esencial del derecho fundamental restringido (STC 292/2000, FJ 11)²⁰¹.

Ahora bien, si la Ley es la única habilitada por la Constitución para fijar los límites a los derechos fundamentales y, en este caso, al de protección de datos, y esos límites no pueden ser distintos a los constitucionalmente previstos (que para el caso no son otros que los derivados de la coexistencia de este derecho fundamental con otros derechos y bienes jurídicos de rango constitucional), entonces el apoderamiento legal que permita a un Poder Público recoger, almacenar, tratar, usar y, en su caso, ceder datos personales, sólo está justificado si responde a la protección de otros derechos fundamentales o bienes constitucionalmente protegidos (STC 292/2000, FJ 11).

Por tanto, si aquellas operaciones con los datos personales de una persona no se realizan con estricta observancia de las normas que lo regulan, se vulnera el derecho a la protección de datos, pues se le imponen límites constitucionalmente ilegítimos, ya sea a su contenido o a su ejercicio. Asimismo, lo conculcará esa ley limitativa si regula los límites de forma tal que hagan impracticable el derecho fundamental afectado o ineficaz la garantía que la Constitución le otorga. Y también lo hará aquella ley que se limita a apoderar a otro Poder Público para

²⁰⁰ Esto lo puede hacer el legislador ordinario a tenor de lo dispuesto en el art. 53.1 CE (STC 292/2000, FJ 11).

²⁰¹ SSTC 57/1994 de 28 de febrero, FJ 6; 18/1999 de 22 de febrero, FJ 2.

fijar las restricciones que puedan imponerse a los derechos fundamentales, esgrimiendo incluso intereses que no son protegidos constitucionalmente²⁰².

La fijación de los límites de un derecho fundamental no es un lugar idóneo para la colaboración entre la Ley y las normas infralegales, pues esta posibilidad de colaboración debe quedar reducida a los casos en los que, por exigencias prácticas, las regulaciones infralegales sean las idóneas para fijar aspectos de carácter secundario y auxiliares de la regulación legal del ejercicio de los derechos fundamentales, siempre con sujeción a la ley pertinente (STC 292/2000, FJ 11)²⁰³.

Más concretamente y en relación con el derecho a la intimidad, se ha puesto de relieve no sólo la necesidad de que sus posibles limitaciones estén fundadas en una previsión legal que tenga justificación constitucional y que sean proporcionadas, sino que la Ley que restrinja este derecho debe expresar con precisión todos y cada uno de los presupuestos materiales de la medida limitadora²⁰⁴. De no ser así, mal cabe entender que la resolución judicial o el acto administrativo que la aplique estén fundados en la Ley, ya que lo que ésta ha

²⁰² Será así cuando la Ley, que debe regular los límites a los derechos fundamentales con escrupuloso respeto a su contenido esencial, se limita a apoderar a otro Poder Público para fijar en cada caso las restricciones que pueden imponerse a los derechos fundamentales, cuya singular determinación y aplicación estará al albur de las decisiones que adopte ese Poder Público, quien podrá decidir, en lo que ahora nos interesa, sobre la obtención, almacenamiento, tratamiento, uso y cesión de datos personales en los casos que estime convenientes y esgrimiendo, incluso, intereses o bienes que no son protegidos con rango constitucional. De ser ese el caso, la Ley habrá vulnerado el derecho fundamental en cuestión, ya que no sólo habrá frustrado la función de garantía propia de toda reserva de ley relativa a derechos fundamentales al renunciar a fijar por sí misma esos límites, dado que la reserva de Ley impone al legislador, además de promulgar esa Ley, regular efectivamente en ella la materia objeto de la reserva; sino también al permitir que el derecho fundamental ceda ante intereses o bienes jurídicos de rango infraconstitucional en contra de lo dispuesto en la propia Constitución, que no lo prevé así. Por esta razón, cuando la Constitución no contempla esta posibilidad de que un Poder Público distinto al legislador fije y aplique los límites de un derecho fundamental o que esos límites sean distintos a los implícitamente derivados de su coexistencia con los restantes derechos y bienes constitucionalmente protegidos, es irrelevante que la Ley habilitante sujete a los Poderes Públicos en ese cometido a procedimientos y criterios todo lo precisos que se quiera, incluso si la Ley habilitante enumera con detalle los bienes o intereses invocables por los Poderes Públicos en cuestión, o que sus decisiones sean revisables jurisdiccionalmente (que lo son en cualquier caso, con arreglo al art. 106 CE). Esa Ley habrá infringido el derecho fundamental porque no ha cumplido con el mandato contenido en la reserva de ley, al haber renunciado a regular la materia que se le ha reservado, remitiendo ese cometido a otro Poder Público, frustrando así una de las garantías capitales de los derechos fundamentales en el Estado democrático y social de Derecho (art. 1.1 CE) (STC 292/2000, FJ 11).

²⁰³ SSTC 83/1984, FJ 4; 137/1986, FJ 3 y 254/1994, FJ 5.

²⁰⁴ SSTC 110/1984, FJ 3 y 254/1993, FJ 7.

hecho, haciendo dejación de sus funciones, es apoderar a otros Poderes Públicos para que sean ellos quienes fijen los límites al derecho fundamental (STC 292/2000, FJ 16).

De igual modo, respecto al derecho a la protección de datos personales cabe estimar que la legitimidad constitucional de la restricción de este derecho no puede estar basada, por sí sola, en la actividad de la Administración Pública. Ni es suficiente que la Ley apodere a ésta para que precise en cada caso sus límites, limitándose a indicar que deberá hacer tal precisión cuando concurra algún derecho o bien constitucionalmente protegido. Es el legislador quien debe determinar cuándo concurre ese bien o derecho que justifica la restricción del derecho a la protección de datos personales y en qué circunstancias puede limitarse y, además, es él quien debe hacerlo mediante reglas precisas que hagan previsible al interesado la imposición de tal limitación y sus consecuencias. Pues en otro caso el legislador habría trasladado a la Administración el desempeño de una función que sólo a él compete en materia de derechos fundamentales en virtud de la reserva de Ley del art. 53.1 CE, esto es, establecer claramente el límite y su regulación (STC 292/2000, FJ 16).

El TEDH ha indicado que se produce una lesión del derecho garantizado por el art. 8 CEDH cuando se recogen, almacenan y usan datos personales si, a pesar de existir una previsión legal, la norma que prevé estos procedimientos no establece las garantías necesarias. En este Sentido dice el Tribunal, la ley que permita la injerencia debe ser clara y concisa y debe establecer bajo qué circunstancias se produce la medida, por ejemplo: el procedimiento que se va a seguir, la información que va a ser recogida o almacenada (por cuánto tiempo y bajo qué condiciones), los procedimientos de acceso y cesión de datos, etc. (Arenas Ramiro, 2008: 139).

En cuanto a los límites constitucionales, el art. 105 b) CE, refiere que la ley regulará el acceso de los ciudadanos a los archivos y registros administrativos, salvo en lo que afecte a la seguridad y defensa del Estado, la averiguación de los delitos y la intimidad de las personas. El TEDH en aplicación del art. 8 CEDH (aplicable también al tráfico de datos de carácter personal),

también ha tenido en cuenta estos límites, al reconocer que lo podrán ser los relativos a la seguridad nacional²⁰⁵ o la persecución de infracciones penales²⁰⁶; y ha exigido que los mismos estén previstos legalmente y sean los indispensables en una sociedad democrática²⁰⁷. Lo que implica que la ley que establezca esos límites sea accesible al individuo concernido por ella, que resulten previsibles las consecuencias que para él pueda tener su aplicación, y que los límites respondan a una necesidad social imperiosa y sean adecuados y proporcionados para el logro de su propósito (STC 292/2000, FJ 9)²⁰⁸.

4. Principios en el tratamiento

La recogida y tratamiento de datos deberá regirse por los principios contenidos en la LOPD, y el art. 4.1 de esta Ley distingue entre ambos conceptos, aunque se trata de una distinción que desde un punto de vista jurídico resulta difusa, ya que el art. 3.c) LOPD al definir el tratamiento de datos hace mención de la recogida de datos.

Para que se pueda ejercer el derecho a la protección de datos personales no basta la presencia de datos de carácter personal, ya que tiene que haber tratamiento de datos personales. Este derecho no protege a los datos, ya que estos por sí mismos no constituyen un riesgo, el peligro surge cuando son tratados. Por tanto, para que entre en juego el derecho fundamental a la protección de datos es necesario que estos se hallen registrados en un soporte físico que los haga susceptibles de tratamiento. Si no hay tratamiento no hay derecho fundamental a la protección de datos, aunque puede haber un derecho a la intimidad (Troncoso Reigada, 2008: 43-44).

²⁰⁵ STEDH caso *Leander* de 26 de marzo de 1987, §§ 47 y sigs.

²⁰⁶ *Mutatis mutandis*, SSTEDH, casos *Z* de 25 de febrero de 1997 y *Funke* de 25 de febrero de 1993.

²⁰⁷ El art. 8.2 CEDH dice que no podrá haber injerencia de la autoridad pública en el ejercicio del derecho al respeto a la vida privada y familiar, 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 de las infracciones penales, la protección de la salud o de la moral, o la protección de los derechos y las libertades de los demás.

²⁰⁸ SSTEDH, caso *X e Y* de 26 de marzo de 1985; caso *Leander* de 26 de marzo de 1987; caso *Gaskin* de 7 de julio de 1989; *mutatis mutandis*, caso *Funke* de 25 de febrero de 1993 y caso *Z* de 25 de febrero de 1997.

a) Tratamiento

El tratamiento de datos es definido por la LOPD como las operaciones y procedimientos técnicos de carácter automatizado o no, que permitan la recogida, grabación, conservación, elaboración, modificación, bloqueo y cancelación, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias.

b) Recogida de datos

La recogida de datos hace referencia a cualquier procedimiento en virtud del cual los datos del afectado llegan al conocimiento y disponibilidad del responsable del fichero²⁰⁹. También se puede definir como la comunicación de los datos por el interesado al responsable del fichero o la obtención de dichos datos por otros medios distintos del propio afectado. Los procedimientos de recogida de datos pueden ser diversos: declaraciones o formularios, encuestas o entrevistas, transmisión electrónica de datos, directorios electrónicos o comerciales, páginas Web, etc. (Lesmes Serrano, 2008: 142, 167).

c) Principios

Los principios del derecho a la protección de datos personales, tienen su origen en el Convenio 108 del Consejo de Europa, el cual no se limitó a establecer los principios básicos para la protección de los datos tratados automáticamente -especialmente en sus arts. 5, 6, 7 y 11-, sino que los completó con unas garantías para las personas concernidas, que formula detalladamente su art. 8 (STC 254/1993, de 20 de julio, FJ 4).

La LOPD enuncia en sus arts. 4 a 12 los principios de la protección de datos: calidad de los datos, información previa, consentimiento, atención a los datos especialmente protegidos, seguridad de los datos, deber de secreto, comunicación de los datos y acceso a los datos por cuentas de terceros²¹⁰.

²⁰⁹ Entendiendo por responsable del fichero o tratamiento, a la persona física o jurídica, de naturaleza pública o privada, u órgano administrativo, de decida sobre la finalidad, contenido y uso del tratamiento (art. 3.d LOPD).

²¹⁰ Los principios de protección de datos encuentran su desarrollo en el Título II del RD 1720/2007, arts. 8 a 19. En cuanto a los principios genera les de protección de datos personales se

Estos principios sirven para delimitar el marco en el que debe desenvolverse cualquier uso o cesión de los datos de carácter personal y para integrar la definición de los tipos de infracción definidos en el art. 44 LOPD, pues este precepto aborda la tipificación de las distintas infracciones mediante una remisión a los principios definidos en la propia Ley²¹¹.

4.1 Calidad de los datos

El art. 4 LOPD refiere que el principio de calidad de los datos deberá prever los siguientes siete supuestos:

1. Los datos de carácter personal sólo se podrán recoger para su tratamiento, así como someterlos a dicho tratamiento, cuando sean adecuados, pertinentes y no excesivos en relación con el ámbito y las finalidades determinadas, explícitas y legítimas para las que se hayan obtenido.
2. Los datos de carácter personal objeto de tratamiento no podrán usarse para finalidades incompatibles con aquellas para las que los datos hubieran sido recogidos. No se considerará incompatible el tratamiento posterior de estos con fines históricos, estadísticos o científicos.
3. Los datos de carácter personal serán exactos y puestos al día de forma que respondan con veracidad a la situación actual del afectado.
4. Si los datos de carácter personal registrados resultaran ser inexactos, en todo o en parte, o incompletos, serán cancelados y sustituidos de oficio por los correspondientes datos rectificadas o completados, sin perjuicio de las facultades que a los afectados reconoce el artículo 16.
5. Los datos de carácter personal serán cancelados cuando hayan dejado de ser necesarios o pertinentes para la finalidad para la cual hubieran sido recabados o registrados. No serán conservados en forma que permita la identificación del interesado durante un período superior al necesario para los fines en base a los cuales hubieran sido recabados o registrados.

puede consultar a Gozáni (2002: 45 y ss.), Lesmes Serrano (2008: 138-323), Díaz-Arias (2008: 33-62), entre otros.

²¹¹ Sentencia de la Audiencia Nacional, Sección 1ª, de 25 de julio de 2006 (rec. 210/2005), FJ 3.

Reglamentariamente se determinará el procedimiento por el que, por excepción, atendidos los valores históricos, estadísticos o científicos de acuerdo con la legislación específica, se decida el mantenimiento íntegro de determinados datos.

6. Los datos de carácter personal serán almacenados de forma que permitan el ejercicio del derecho de acceso, salvo que sean legalmente cancelados.
7. Se prohíbe la recogida de datos por medios fraudulentos, desleales o ilícitos.

El principio de calidad de los datos contenido en la LOPD es interesante porque comprende aquellos previstos en el Convenio 108 del Consejo de Europa. El art. 5 del Convenio 108 contempla la Calidad de los datos y en este se prevén los principios de lealtad, licitud, finalidad, pertinencia, proporcionalidad, exactitud o veracidad y conservación. Asimismo, el art. 6 del citado Convenio refiere el principio de atención a datos especialmente protegidos. El art. 7 del Convenio toma en cuenta el principio de seguridad de los datos y el art. 8 considera el principio de acceso, rectificación y cancelación de los datos, así como el disponer de un recurso. Por otro lado, la Directiva 95/46/CE además de prever los principios contenidos en el Convenio contempla el consentimiento y la legitimidad (en cuanto al fin y en lo que hace al tratamiento de los datos).

El que la Directiva y el Convenio no sean homogéneos en los principios ha propiciado la crítica en la doctrina, que entiende que el amplio margen de actuación dejado en manos de los Estados provoca la existencia de regulaciones más estrictas en un Estado que en otro. En cualquier caso, el TJCE se ha pronunciado sobre tal posibilidad y ha señalado que en tanto no se obstaculice la libre circulación de datos personales entre los Estados miembros de la Unión, no existe ningún problema porque un Estado miembro otorgue una mayor protección a los datos personales (Arenas Ramiro, 2008: 317).

El principio de calidad de los datos está compuesto por varios principios que se pueden desglosar así:

a) Principio de pertinencia y proporcionalidad

Los datos de carácter personal sólo se podrán recoger para su tratamiento, así como someterlos a dicho tratamiento, cuando sean adecuados, pertinentes y no excesivos en relación con el ámbito y las finalidades determinadas, explícitas y legítimas para las que se hayan obtenido.

b) Principio de Finalidad

Los datos de carácter personal objeto de tratamiento no podrán usarse para finalidades incompatibles con aquellas para las que los datos hubieran sido recogidos. No se considerará incompatible el tratamiento posterior de estos con fines históricos, estadísticos o científicos.

c) Principio de exactitud o veracidad.

Los datos de carácter personal serán exactos y puestos al día de forma que respondan con veracidad a la situación actual del afectado. Si los datos de carácter personal registrados resultaran ser inexactos, en todo o en parte, o incompletos, serán cancelados y sustituidos de oficio por los correspondientes datos rectificadas o completados, sin perjuicio de las facultades que a los afectados reconoce el artículo 16 LOPD.

d) Principio de conservación.

Los datos de carácter personal serán cancelados cuando hayan dejado de ser necesarios o pertinentes para la finalidad para la cual hubieran sido recabados o registrados. No serán conservados en forma que permita la identificación del interesado durante un período superior al necesario para los fines en base a los cuales hubieran sido recabados o registrados. Reglamentariamente se determinará el procedimiento por el que, por excepción, atendidos los valores históricos, estadísticos o científicos de acuerdo con la legislación específica, se decida el mantenimiento íntegro de determinados datos.

e) Principio de acceso.

Los datos de carácter personal serán almacenados de forma que permitan el ejercicio del derecho de acceso²¹², salvo que sean legalmente cancelados.

f) Principio de lealtad y licitud.

Se prohíbe la recogida de datos por medios fraudulentos, desleales o ilícitos.

4.2 Información previa

El art. 5 LOPD hace referencia al derecho a la información previa en la recogida de datos. Los interesados a los que se soliciten datos personales deberán ser previamente informados de modo expreso, preciso e inequívoco: a) de la existencia de un fichero o tratamiento de datos de carácter personal, de la finalidad de la recogida de estos y de los destinatarios de la información; b) del carácter obligatorio o facultativo de su respuesta a las preguntas que les sean planteadas, c) de las consecuencias de la obtención de los datos o de la negativa a suministrarlos; d) de la posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición; y e) de la identidad y dirección del responsable del tratamiento o, en su caso, de su representante²¹³.

Cuando los datos de carácter personal no hayan sido recabados del interesado, éste deberá ser informado de forma expresa, precisa e inequívoca, por el responsable del fichero o su representante, dentro de los tres meses siguientes al momento del registro de los datos, salvo que ya hubiera sido informado con anterioridad, del contenido del tratamiento, de la procedencia de los datos, así como de lo previsto en las letras a), d) y e). Esto, no será de aplicación cuando expresamente una Ley lo prevea, cuando el tratamiento tenga fines históricos, estadísticos o científicos, o cuando la información al interesado resulte imposible

²¹² El art. 15 LOPD regula el derecho de acceso. Para mayor abundamiento ver este derecho en el apartado de los derechos de las personas.

²¹³ Cuando el responsable del tratamiento no esté establecido en el territorio de la Unión Europea y utilice en el tratamiento de datos medios situados en territorio español, deberá designar, salvo que tales medios se utilicen con fines de tránsito, un representante en España, sin perjuicio de las acciones que pudieran emprenderse contra el propio responsable del tratamiento. Cuando se utilicen cuestionarios u otros impresos para la recogida, figurarán en los mismos, en forma claramente legible, las advertencias a que se refieren cada uno de los incisos. No será necesaria la información a que se refieren las letras b), c) y d) si el contenido de ella se deduce claramente de la naturaleza de los datos personales que se solicitan o de las circunstancias en que se recaban.

o exija esfuerzos desproporcionados, a criterio de la Agencia de Protección de Datos o del organismo autonómico equivalente, en consideración al número de interesados, a la antigüedad de los datos y a las posibles medidas compensatorias²¹⁴. Así tampoco, cuando los datos procedan de fuentes accesibles al público y se destinen a la actividad de publicidad o prospección comercial, en cuyo caso, en cada comunicación que se dirija al interesado se le informará del origen de los datos y de la identidad del responsable del tratamiento así como de los derechos que le asisten.

Es particularmente interesante, lo que refiere el dispositivo anterior, en cuanto a las excepciones que habrán de hacerse al momento de informar al interesado el manejo de sus datos personales (ficheros con fines históricos, estadísticos o científicos, o cuando el informar implique esfuerzos desproporcionados)²¹⁵. Señalando que el ejercicio del principio de información tampoco será necesario cuando los datos no sean recopilados directamente del interesado y procedan de fuentes públicas²¹⁶; sin embargo, precisa que si adicionalmente se utilizan con fines publicitarios, en dicho caso, si habrá de informarse en cada comunicación al interesado, del origen de los datos, de la identidad del responsable del fichero y de los derechos que se pueden ejercitar.

El derecho a la información es capital en la protección de datos personales, ya que se debe proporcionar información clara y comprensible para cualquier usuario respecto de qué tratamientos se van a realizar con sus datos, finalidad y el responsable de los mismos, así como de los destinatarios de la

²¹⁴ El 18 de abril de 2012 fueron publicados en el DOF los “Criterios Generales para la instrumentación de medidas compensatorias sin la autorización expresa del IFAI”.

²¹⁵ Entonces no se habrá de informar de: 1) de la existencia de un fichero o tratamiento de datos de carácter personal, de la finalidad de la recogida de estos y de los destinatarios de la información; 2) de la posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición; y 3) de la identidad y dirección del responsable del tratamiento o, en su caso, de su representante.

²¹⁶ Las fuentes accesibles al público son aquellos ficheros cuya consulta puede ser realizada por cualquier persona, no impedida por una norma limitativa, o sin más exigencia que, en su caso, el abono de una contraprestación. Tienen la consideración de fuentes de acceso público, exclusivamente: a) el censo promocional; b) los repertorios telefónicos en los términos previstos por su normativa específica (Véase: Real Decreto 424/2005, de 15 de Abril); c) las listas de personas pertenecientes a grupos de profesionales que contengan únicamente los datos de nombre, título, profesión, actividad, grado académico, dirección e indicación de su pertenencia al grupo; d) los Diarios y boletines oficiales; y e) los medios de comunicación (art. 3.j LOPD). Véase: Veleiro (2008: 58).

información personal obtenida y de la posibilidad y procedimiento para ejercer los derechos de acceso, rectificación-cancelación y oposición (Aced Félez, 2000: 118).

En los supuestos en que se produzca una modificación del responsable del fichero como consecuencia de una operación de fusión, escisión, cesión global de activos y pasivos, aportación o transmisión de negocio o rama de actividad empresarial, o cualquier operación de reestructuración societaria de análoga naturaleza, contemplada por la normativa mercantil, no se producirá cesión de datos, sin perjuicio del cumplimiento por el responsable de lo dispuesto en el art. 5 LOPD (art. 19 RD 1720/2007).

La STC 292/2000 ha señalado que son elementos característicos de la definición constitucional del derecho fundamental a la protección de datos personales los derechos del afectado a consentir sobre al recogida y uso de sus datos personales y a saber de los mismos y que es evidente que el interesado debe ser informado tanto de la posibilidad de cesión de sus datos personales y sus circunstancias como del destino de estos, pues sólo así será eficaz su derecho a consentir, en cuanto facultad esencial de su derecho a controlar y disponer de sus datos personales.

4.3 Consentimiento

Según el art. 3.h LOPD define al consentimiento del interesado como toda manifestación de voluntad, libre, inequívoca, específica e informada, mediante la que el interesado consienta el tratamiento de datos personales que le conciernen. Así el art. 6 LOPD establece respecto del consentimiento del afectado que:

1. El tratamiento de los datos de carácter personal requerirá el consentimiento inequívoco del afectado, salvo que la Ley disponga otra cosa.
2. No será preciso el consentimiento cuando los datos de carácter personal se recojan para el ejercicio de las funciones propias de las Administraciones Públicas en el ámbito de sus competencias; cuando se refieran a las partes de un contrato o precontrato de una relación negocial, laboral o

administrativa y sean necesarios para su mantenimiento o cumplimiento; cuando el tratamiento de los datos tenga por finalidad proteger un interés vital del interesado en los términos del artículo 7 apartado 6 de la presente Ley²¹⁷, o cuando los datos figuren en fuentes accesibles al público y su tratamiento sea necesario para la satisfacción del interés legítimo perseguido por el responsable del fichero o por el del tercero a quien se comuniquen los datos, siempre que no se vulneren los derechos y libertades fundamentales del interesado.

3. El consentimiento a que se refiere el artículo podrá ser revocado cuando exista causa justificada para ello y no se le atribuyan efectos retroactivos.
4. En los casos en los que no sea necesario el consentimiento del afectado para el tratamiento de los datos de carácter personal, y siempre que una Ley no disponga lo contrario, éste podrá oponerse a su tratamiento cuando existan motivos fundados y legítimos relativos a una concreta situación personal. En tal supuesto, el responsable del fichero excluirá del tratamiento los datos relativos al afectado.

En cuanto a la recogida y tratamiento para fines policiales de datos personales por las Fuerzas y Cuerpos de Seguridad sin consentimiento de las personas afectadas, están limitados a aquellos supuestos y categorías de datos que resulten necesarios para la prevención de un peligro real para la seguridad pública o para la represión de infracciones penales (art. 22.2 LOPD).

El responsable del tratamiento deberá obtener el consentimiento del interesado para el tratamiento de sus datos, salvo en los casos que no sea exigible según lo dispuesto por la Ley. La solicitud del consentimiento deberá ir referida a un tratamiento o serie de tratamientos concretos, con delimitación de la finalidad para los que se recaba, así como de las restantes condiciones que concurran en el

²¹⁷ El art. 7.6 LOPD cita: No obstante lo dispuesto en los apartados anteriores, podrán ser objeto de tratamiento los datos de carácter personal a que se refieren los apartados 2 y 3 de este artículo, cuando dicho tratamiento resulte necesario para la prevención o para el diagnóstico médico, la prestación de asistencia sanitaria o tratamientos médicos o la gestión de servicios sanitarios, siempre que dicho tratamiento de datos se realice por un profesional sanitario sujeto al secreto profesional o por otra persona sujeta asimismo a una obligación equivalente de secreto.

tratamiento o serie de tratamientos²¹⁸. Corresponderá al responsable del tratamiento la prueba de la existencia del consentimiento del afectado por cualquier medio de prueba admisible en derecho (art. 12 RD 1720/2007).

En cuanto al consentimiento para el tratamiento de datos de menores de edad, se establece que podrá procederse al tratamiento de los datos de los mayores de catorce años con su consentimiento, salvo en aquellos casos en los que la Ley exija para su prestación la asistencia de los titulares de la patria potestad o tutela. En el caso de los menores de catorce años se requerirá el consentimiento de los padres o tutores. En ningún caso podrán recabarse del menor datos que permitan obtener información sobre los demás miembros del grupo familiar, o sobre las características del mismo, como los datos relativos a la actividad profesional de los progenitores, información económica, datos sociológicos o cualesquiera otros, sin el consentimiento de los titulares de tales datos²¹⁹ (art. 13 RD 1720/2007).

El afectado podrá revocar su consentimiento a través de un medio sencillo, gratuito y que no implique ingreso alguno para el responsable del fichero o tratamiento. En particular, se considerara apropiado el procedimiento en el que tal negativa pueda efectuarse, entre otros, mediante un envío prefranqueado al responsable del tratamiento o la llamada a un número telefónico gratuito o a los servicios de atención al público que el mismo hubiera establecido²²⁰. Cuando el interesado hubiera solicitado del responsable del tratamiento la confirmación del cese en el tratamiento de sus datos, éste deberá responder expresamente a su solicitud (art. 17 RD 1720/2007).

4.4 Atención a datos especialmente protegidos

En cuanto a este principio el art. 7 LOPD refiere que nadie podrá ser obligado a declarar sobre su ideología, religión o creencias²²¹ y que sólo con el

²¹⁸ El art. 14 RD 1720/2007 establece la forma en que se deberá recabar el consentimiento.

²¹⁹ No obstante, podrán recabarse los datos de identidad y dirección del padre, madre o tutor con la única finalidad de recabar la autorización prevista en la primera parte del párrafo.

²²⁰ El responsable cesará en el tratamiento de los datos en el plazo máximo de diez días a contar desde el de la recepción de la revocación del consentimiento.

²²¹ Cuando en relación con estos datos se proceda a recabar este consentimiento se advertirá al interesado acerca de su derecho a no prestarlo.

consentimiento expreso y por escrito del afectado podrán ser objeto de tratamiento los datos de carácter personal que revelen la ideología, afiliación sindical, religión y creencias²²². Los datos de carácter personal que hagan referencia al origen racial, a la salud y a la vida sexual sólo podrán ser recabados, tratados y cedidos cuando, por razones de interés general, así lo disponga una Ley o el afectado consienta expresamente; quedando prohibidos los ficheros creados con la finalidad exclusiva de almacenar datos de carácter personal que revelen la ideología, afiliación sindical, religión, creencias, origen racial o étnico, o vida sexual.

Este dispositivo también señala que los datos de carácter personal relativos a la comisión de infracciones penales o administrativas sólo podrán ser incluidos en ficheros de las Administraciones Públicas competentes en los supuestos previstos en las respectivas normas reguladoras. Y que no obstante lo dispuesto en los apartados del art. 7 LOPD podrán ser objeto de tratamiento los datos de carácter personal a que se refieren los apartados 2 y 3 de este artículo²²³, cuando dicho tratamiento resulte necesario para la prevención o para el diagnóstico médicos, la prestación de asistencia sanitaria o tratamientos médicos o la gestión de servicios sanitarios, siempre que dicho tratamiento de datos se realice por un profesional sanitario sujeto al secreto profesional o por otra persona sujeta asimismo a una obligación equivalente de secreto. También podrán ser objeto de tratamiento los datos cuando sea necesario para salvaguardar el interés vital del afectado o de otra persona, en el supuesto de que el afectado esté física o jurídicamente incapacitado para dar su consentimiento.

²²² Se exceptúan los ficheros mantenidos por los partidos políticos, sindicatos, iglesias, confesiones o comunidades religiosas y asociaciones, fundaciones y otras entidades sin ánimo de lucro, cuya finalidad sea política, filosófica, religiosa o sindical, en cuanto a los datos relativos a sus asociados o miembros, sin perjuicio de que la cesión de dichos datos precisará siempre el previo consentimiento del afectado.

²²³ 2. Sólo con el consentimiento expreso y por escrito del afectado podrán ser objeto de tratamiento los datos de carácter personal que revelen la ideología, afiliación sindical, religión y creencias. Se exceptúan los ficheros mantenidos por los partidos políticos, sindicatos, iglesias, confesiones o comunidades religiosas y asociaciones, fundaciones y otras entidades sin ánimo de lucro, cuya finalidad sea política, filosófica, religiosa o sindical, en cuanto a los datos relativos a sus asociados o miembros, sin perjuicio de que la cesión de dichos datos precisará siempre el previo consentimiento del afectado; y 3. Los datos de carácter personal que hagan referencia al origen racial, a la salud y a la vida sexual sólo podrán ser recabados, tratados y cedidos cuando, por razones de interés general, así lo disponga una ley o el afectado consienta expresamente.

En lo que hace a los datos relativos a la salud, el art. 8 LOPD dice que sin perjuicio de lo que se dispone en el art. 11 LOPD respecto de la cesión, las instituciones y los centros sanitarios públicos y privados y los profesionales correspondientes podrán proceder al tratamiento de los datos de carácter personal relativos a la salud de las personas que a ellos acudan o hayan de ser tratados en los mismos, de acuerdo con lo dispuesto en la legislación estatal o autonómica sobre sanidad.

En cuanto a la recogida y tratamiento para fines policiales de datos personales por las Fuerzas y Cuerpos de Seguridad sin consentimiento de las personas afectadas están limitados a aquellos supuestos y categorías de datos que resulten necesarios para la prevención de un peligro real para la seguridad pública o para la represión de infracciones penales, debiendo ser almacenados en ficheros específicos establecidos al efecto, que deberán clasificarse por categorías en función de su grado de fiabilidad (art. 22.2 LOPD).

La recogida y tratamiento por las Fuerzas y Cuerpos de Seguridad de los datos, a que hacen referencia los apartados 2 y 3 del art. 7 LOPD²²⁴, podrán realizarse exclusivamente en los supuestos en que sea absolutamente necesario para los fines de una investigación concreta, sin perjuicio del control de legalidad de la actuación administrativa o de la obligación de resolver las pretensiones formuladas en su caso por los interesados que corresponden a los órganos jurisdiccionales (art. 22.3 LOPD)²²⁵.

En cuanto a los ficheros establecidos para la investigación del terrorismo y de formas graves de delincuencia organizada, el régimen de protección de datos que establece la LOPD no será aplicable. No obstante, en estos supuestos el

²²⁴ Dichos apartados citan: 2. Sólo con el consentimiento expreso y por escrito del afectado podrán ser objeto de tratamiento los datos de carácter personal que revelen la ideología, afiliación sindical, religión y creencias. Se exceptúan los ficheros mantenidos por los partidos políticos, sindicatos, iglesias, confesiones o comunidades religiosas y asociaciones, fundaciones y otras entidades sin ánimo de lucro, cuya finalidad sea política, filosófica, religiosa o sindical, en cuanto a los datos relativos a sus asociados o miembros, sin perjuicio de que la cesión de dichos datos precisará siempre el previo consentimiento del afectado. 3. Los datos de carácter personal que hagan referencia al origen racial, a la salud y a la vida sexual sólo podrán ser recabados, tratados y cedidos cuando, por razones de interés general, así lo disponga una ley o el afectado consienta expresamente.

²²⁵ Para mayor abundamiento, véase los comentarios al art. 22 LOPD de Esquinas Valverde (2010: 148 a 150).

responsable del fichero comunicará previamente la existencia del mismo, sus características generales y su finalidad a la Agencia de Protección de datos (art. 2.2.c LOPD).

4.5 Seguridad

Por seguridad de las redes y de la información –por tanto de los datos de carácter personal- se entiende la capacidad de las redes o de los sistemas de información de resistir, con un determinado nivel de confianza, los accidentes o acciones ilícitas o malintencionadas que comprometan la disponibilidad, autenticidad, integridad y confidencialidad de los datos almacenados o transmitidos y de los servicios que dichas redes y sistemas ofrecen²²⁶.

El art. 9 LOPD sobre la seguridad de los datos establece que:

1. El responsable del fichero, y, en su caso, el encargado del tratamiento, deberán adoptar las medidas de índole técnica y organizativas necesarias que garanticen la seguridad de los datos de carácter personal y eviten su alteración, pérdida, tratamiento o acceso no autorizado, habida cuenta del estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a que están expuestos, ya provengan de la acción humana o del medio físico o natural²²⁷.
2. No se registrarán datos de carácter personal en ficheros que no reúnan las condiciones que se determinen por vía reglamentaria con respecto a su integridad y seguridad y a las de los centros de tratamiento, locales, equipos, sistemas y programas.
3. Reglamentariamente se establecerán los requisitos y condiciones que deban reunir los ficheros y las personas que intervengan en el tratamiento de los datos a que se refiere el art. 7 LOPD.

²²⁶ Art. 4.c del Reglamento (CE) nº 460/2004 del Parlamento Europeo y del Consejo, de 10 de marzo de 2004, por el que se crea la Agencia Europea de Seguridad de las Redes y de la Información.

²²⁷ El tema de las medidas de seguridad es bastante amplio y es motivo de una investigación exhaustiva y muy técnica. Para mayor abundamiento en las medidas de seguridad a implementar por el encargado del tratamiento véase a Santamaría Ramos (2011: 163 – 243).

Las medidas de seguridad en el tratamiento de datos de carácter personal se encuentran desarrolladas en los arts. 79 a 114 del RD 1720/2007, así mismo precisa diferentes protocolos de seguridad para ficheros de tratamiento automatizado y para los no automatizados. Las medidas exigibles a los ficheros y tratamientos se clasifican en tres niveles: básico, medio y alto, su ámbito de aplicación es el siguiente²²⁸:

- Nivel básico: todos los ficheros o tratamientos de datos deberán adoptar las medidas de seguridad de nivel básico, debiendo implementarse también el nivel medio y/o alto si corresponde según la información que se trate.
- Nivel medio: ficheros que contengan datos relativos a la comisión de infracciones administrativas o penales, de solvencia patrimonial y crédito, de los tributarios o financieros, de los que sean responsables las entidades Gestoras y Servicios Comunes de la Seguridad Social y las mutuas de accidentes de trabajo y enfermedades profesionales, y de aquellos que contengan un conjunto de datos de carácter personal que ofrezcan una definición de las características o de la personalidad de los ciudadano y que permitan evaluar determinados aspectos de la personalidad o del comportamientos de los mismos.
- Nivel alto: ficheros que contengan datos que se refieran a ideología, afiliación sindical, religión, creencias, origen racial, salud o vida sexual. También a los que se refieran a datos recabados para fines policiales sin consentimiento de las personas afectadas y aquellos que precisen datos derivados de actos de violencia de género.

Muchos de los casos relacionados con la infracción de medidas de seguridad tienen que ver con la aparición en la vía pública de documentos que contenían datos personales de uso interno en determinadas empresas y entidades,

²²⁸ Art. 81 RD 1720/2007. Por otro lado hemos de mencionar que los niveles de seguridad son acumulativos, por lo que las medidas de seguridad de nivel básico son exigibles en todos los casos, mientras que las medidas de nivel medio complementan a las anteriores en el caso de ficheros clasificados en este nivel, y que las de nivel alto, cuando deban adoptarse, incluyen también las de nivel básico y medio.

en los que la Audiencia Nacional ha fallado que efectivamente estas últimas no habían prestado la diligencia necesaria en orden a la observancia de las medidas de seguridad y que éstas no habían sido las adecuadas²²⁹ (Lesmes Serrano, 2008: 266-268).

4.6 Deber de secreto

El art. 10 LOPD en cuanto al deber de secreto refiere que el responsable del fichero y quienes intervengan en cualquier fase del tratamiento de los datos de carácter personal están obligados al secreto profesional respecto de los mismos y al deber de guardarlos, obligaciones que subsistirán aun después de finalizar sus relaciones con el titular del fichero o, en su caso, con el responsable del mismo.

En cuanto a las personas que tienen el deber de secreto de los datos personales, es importante recordar las definiciones que la propia ley hace del responsable del fichero y de quienes intervienen en el tratamiento, es decir los encargados del mismo. El responsable del fichero es la persona física o jurídica, de naturaleza pública o privada, u órgano administrativo, que decida sobre la finalidad, contenido y uso del tratamiento. El encargado del tratamiento es 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.

Incumplir este deber de secreto es una infracción *leve*, salvo constituya otro tipo de infracción (art. 44.2.e LOPD). Será constitutivo de infracción *grave* cuando la vulneración de dicho deber sea sobre datos de carácter personal incorporados a ficheros que contengan datos relativos a la comisión de infracciones administrativas o penales, Hacienda Pública, servicios financieros, prestación de servicios de solvencia patrimonial y crédito, así como aquellos otros ficheros que contengan un conjunto de datos de carácter personal suficientes para obtener una evaluación de la personalidad del individuo (art. 44.3.g LOPD). Y será una infracción *muy grave* cuando la vulneración del deber de guardar secreto sea sobre datos que revelen la ideología, afiliación sindical,

²²⁹ SSAN Sección 1ª: rec. 227/2004 de 25 de enero, rec. 119/2005 de 10 de noviembre de 2006, 478/2004 de 23 de marzo de 2006, rec. 1517/2001 de 15 de octubre de 2003.

religión y creencias, o hagan referencia al origen racial, a la salud y a la vida sexual; así como los que hayan sido recabados para fines policiales sin consentimiento de las personas afectadas (art. 44.4.g LOPD).

No siempre el suministro de un dato aislado lleva consigo la infracción del art. 10 LOPD, pues debe estar vinculado a una persona determinada. El deber de secreto no es absoluto, puesto que si lo fuera resultaría imposible la cesión de datos sin consentimiento del afectado prevista en determinados casos según el art. 11 LOPD (Comunicación de los datos) o el acceso a los datos por cuenta de terceros a que se refiere el art. 12 LOPD (Lesmes Serrano, 2008: 272-273).

Se distingue entre el “deber de secreto” que es un concepto más restringido y la “cesión de datos” que implica, además de desvelar datos secretes, un elemento volitivo cualificado, en cuanto que se haya previsto y querido por el responsable del tratamiento que la información que se comunica pueda ser utilizada por tercero(s) con algún fin concreto. En cambio, en la infracción del deber de secreto, hay ausencia de voluntad de que los datos sirvan para ser tratados por el destinatario²³⁰.

La SAN, Sección 1ª, de 3 de noviembre de 2004 (rec. 1160/2002), declara vulnerado el deber de secreto de una entidad bancaria, toda vez que un Juzgado le solicitó la información de movimientos de cuenta corriente de una persona a la que se estaba investigando y la entidad remitió la información a la Policía Nacional y no al Juzgado que era quien la había requerido, además que informa el estado de cuenta con un rango de fechas superior al que se le había solicitado.

4.7 Comunicación de los datos (cesión)

Por cesión o comunicación de datos se entiende, según la Ley, toda revelación de datos realizada a una persona distinta del interesado. Este principio se rige en función del consentimiento del interesado. Así, el art. 11 LOPD regula los casos en que procede o no la comunicación de datos, cuándo no se requiere del consentimiento y en qué casos éste podrá ser revocable o nulo.

²³⁰ SAN, Sección 1ª, de 9 de noviembre de 2005 (rec. 371/2003).

En cuanto a la procedencia, se requerirá del previo consentimiento del interesado, para que los datos de carácter personal objeto del tratamiento puedan ser comunicados a un tercero para el cumplimiento de fines directamente relacionados con las funciones legítimas del cedente y del cesionario. Las *excepciones* a dicho consentimiento tendrán lugar:

- a) Cuando la cesión está autorizada en una Ley.
- b) Cuando se trate de datos recogidos de fuentes accesibles al público.
- c) Cuando el tratamiento responda a la libre y legítima aceptación de una relación jurídica cuyo desarrollo, cumplimiento y control implique necesariamente la conexión de dicho tratamiento con ficheros de terceros. En este caso la comunicación sólo será legítima en cuanto se limite a la finalidad que la justifique.
- d) Cuando la comunicación que deba efectuarse tenga por destinatario al Defensor del Pueblo, el Ministerio Fiscal o los Jueces o Tribunales o el Tribunal de Cuentas, en el ejercicio de las funciones que tiene atribuidas. Tampoco será preciso el consentimiento cuando la comunicación tenga como destinatario a instituciones autonómicas con funciones análogas al Defensor del Pueblo o al Tribunal de Cuentas.
- e) Cuando la cesión se produzca entre Administraciones Públicas y tenga por objeto el tratamiento posterior de los datos con fines históricos, estadísticos o científicos.
- f) Cuando la cesión de datos de carácter personal relativos a la salud sea necesaria para solucionar una urgencia que requiera acceder a un fichero o para realizar los estudios epidemiológicos en los términos establecidos en la legislación sobre sanidad estatal o autonómica.

Será nulo el consentimiento para la comunicación de los datos de carácter personal a un tercero cuando la información que se facilite al interesado no le permita conocer la finalidad a que destinarán los datos cuya comunicación se autoriza o el tipo de actividad de aquél a quien se pretenden comunicar.

Asimismo la ley prevé la revocabilidad del consentimiento para la comunicación, y dice que aquel que reciba alguna información al respecto, por el solo hecho de la comunicación, se obliga a la observancia de las disposiciones de la LOPD. No será de aplicación lo dispuesto por el dispositivo 11 LOPD, cuando la comunicación se efectúe previo procedimiento de disociación.

4.8 Acceso a los datos por cuenta de terceros

El art. 12 LOPD sobre acceso a los datos por cuenta de terceros dice que:

1. No se considerará comunicación de datos el acceso de un tercero a los datos cuando dicho acceso sea necesario para la prestación de un servicio al responsable del tratamiento. La realización de tratamientos por cuenta de terceros deberá estar regulada en un contrato que deberá constar por escrito o en alguna otra forma que permita acreditar su celebración y contenido, estableciéndose expresamente que el encargado del tratamiento únicamente tratará los datos conforme a las instrucciones del responsable del tratamiento, que no los aplicará o utilizará con fin distinto al que figure en dicho contrato, ni los comunicará, ni siquiera para su conservación, a otras personas.
2. En el contrato se estipularán, asimismo, las medidas de seguridad a que se refiere el artículo 9 de esta Ley que el encargado del tratamiento está obligado a implementar.
3. Una vez cumplida la prestación contractual, los datos de carácter personal deberán ser destruidos o devueltos al responsable del tratamiento, al igual que cualquier soporte o documentos en que conste algún dato de carácter personal objeto del tratamiento.
4. En el caso de que el encargado del tratamiento destine los datos a otra finalidad, los comunique o los utilice incumpliendo las estipulaciones del contrato, será considerado, también, responsable del tratamiento, respondiendo de las infracciones en que hubiera incurrido personalmente.

5. Normas reguladoras del tratamiento de datos personales en España

En cuanto a la legislación estatal sobre protección de datos de carácter personal, hemos de señalar que los principales ordenamientos son: la Constitución de España, la LOPD y el RD 1720/2007. Sin embargo, es de precisa que, España cuenta con una amplia legislación en la materia, así como de normas de carácter reglamentario, y ellos sin referir la normativa europea. A continuación, y sólo de una manera ilustrativa, se hace un listado de la normativa estatal vigente²³¹:

a) Legislación estatal

- Constitución Española de 1978.
- Ley:
 - Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.
 - Ley 2/2011, de 4 de marzo, de Economía Sostenible. Modificación de la LOPD. Disposición final quincuagésima sexta.
- Real Decreto:
 - Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal.
 - Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica (DA. 4ª).
 - Real Decreto 1665/2008, de 17 de octubre, por el que se modifica el Estatuto de la Agencia Española de Protección de Datos, aprobado por el Real Decreto 428/1993, de 26 de marzo.

²³¹ Véase también: Agencia de Protección de Datos de la Comunidad de Madrid (2004: 101-223).

- Real Decreto 156/1996, de 2 de febrero, por el que se modifica el Estatuto de la Agencia Española de Protección de Datos.
- Real Decreto 428/1993, de 26 de marzo, por el que se aprueba el Estatuto de la Agencia Española de Protección de Datos.

b) Normas de carácter reglamentario

- Resoluciones:
 - Resolución de 24 de mayo de 2010, de la Agencia Española de Protección de Datos, por la que se regula el Registro Electrónico de la Agencia Española de Protección de Datos.
 - Resolución de 18 de marzo de 2010, de la Agencia Española de Protección de Datos, por la que se crea la Sede Electrónica de la Agencia Española de Protección de Datos.
 - Resolución de marzo de 2011, de la Agencia Española de Protección de Datos, por la que se crea el sello electrónico para su utilización por la Agencia Española de protección de Datos.
 - Resolución de abril de 2011, de la Agencia Española de Protección de Datos, para la utilización de un código seguro de verificación en las actuaciones automatizadas que se hayan publicado su Sede Electrónica.
 - Resolución de 8 de septiembre de 2006, de la Agencia Española de Protección de Datos, por la que se corrigen errores en las Resoluciones de 12 de julio de 2006, por las que se crea el Registro Telemático y se aprueban los formularios electrónicos para inscribir los ficheros en el Registro General de Protección de Datos.
 - Resolución de 1 de septiembre de 2006, de la Agencia Española de Protección de Datos, por la que se determina la información que contiene el Catálogo de ficheros inscritos en el Registro General de Protección de Datos

- Resolución de 12 de julio de 2006, de la Agencia Española de Protección de Datos, por la que se crea el Registro Telemático de la Agencia Española de Protección de Datos.
- Resolución de 12 de julio de 2006, de la Agencia Española de Protección de Datos, por la que se aprueban los formularios electrónicos a través de los que deberán efectuarse las solicitudes de inscripción de ficheros en el Registro General de Protección de Datos, así como los formatos y requerimientos a los que deben ajustarse las notificaciones remitidas en soporte informático o telemático.
- Resolución de 22 de junio de 2001, de la Subsecretaría de Justicia, que concreta el plazo para la implantación de medidas de seguridad de nivel alto.
- Resolución de 30 de mayo de 2000, de la APD, por la que se aprueban los modelos normalizados en soporte papel, magnético y telemático, para la inscripción de los ficheros.
- Instrucciones
 - Instrucción 1/2006, de 12 de diciembre, de la Agencia Española de Protección de Datos sobre el tratamiento de datos personales con fines de vigilancia a través de sistemas de cámaras o videocámaras²³².
 - Instrucción 1/2004, de 22 de diciembre, de la Agencia Española de Protección de Datos sobre publicación de sus Resoluciones.
 - Instrucción 2/1996, de 1 de marzo, de la APD, sobre ficheros automatizados establecidos con la finalidad de controlar el acceso a los casinos y salas de bingo.

²³² Para profundizar en el tema de videovigilancia y protección de datos personales véase a Goñi Sein (2007).

- Instrucción 1/1996, de 1 de marzo, de la APD, sobre ficheros automatizados establecidos con la finalidad de controlar el acceso a los edificios.
- Instrucción 2/1995, de 4 de mayo, de la APD, sobre garantía de los datos personales recabados en la contratación de seguro de vida de forma conjunta con un préstamo hipotecario o personal.

IV. PROTECCION DE DATOS PERSONALES EN MEXICO

El reconocimiento del derecho a la protección de datos personales es relativamente moderno y viene de la mano del desarrollo tecnológico. En la década de los 80's los avances tecnológicos comienzan a permitir que la recogida, almacenamiento y utilización de datos personales (su tratamiento) se lleve a cabo de una forma antes inimaginable. El aumento del número de ordenadores personales, así como su mejora técnica y la conexión entre ellos propicia que se puedan almacenar un mayor número de datos personales, que se produzca con más facilidad la movilidad de los mismos, y por lo tanto, que las posibilidades de su conocimiento por terceros, también sean mayores (Arenas Ramiro, 2006: 83-84).

1. Antecedentes

A diferencia de lo acontecido con otros derechos fundamentales cuyo desarrollo se produjo paralelamente en el ámbito de Europa y Estados Unidos, el derecho a la protección de datos de carácter personal tiene un origen marcadamente europeo. El desarrollo de los primeros estudios en esta materia y la adopción de las primeras legislaciones de protección de datos tienen lugar en Europa (Piñar Mañas, 2003: 39), cuyo origen es el derecho a la intimidad²³³.

Es indudable que el avance de la tecnología ha impulsado lo que hoy se conoce como la *sociedad de la información*, cuyos servicios cubren también aquellos consistentes en transmitir datos a través de una red de comunicación o albergar información facilitada por el destino del servicio (Del Peso Navarro, 2003: 8)²³⁴, es decir, la transferencia de información que ocurre cuando se proporcionan datos personales para un determinado fin o uso.

²³³ Si bien es cierto que las primeras legislaciones de protección de datos aparecen en Europa, también es cierto que el derecho a la intimidad ya se había dado a notar en el célebre artículo de Warren y Brandeis titulado "*The Right to Privacy*". Publicado en Harvard Law Review, vol. IV, núm. 5, 1890. Al respecto véase también a Fioriglio (2008: 46-49).

²³⁴ Internet se ha resistido a ser controlado por organizaciones gubernamentales de cualquier clase. El modelo estatalista no ha podido ser transportado a la gran red. La *domestic analogy* ha sido rechazada como opción organizativa. La autonomía de internet es, en la actualidad, una realidad incontestable y su independencia ha sido mantenida a ultranza y contra la corriente de las tendencias regulatorias establecidas a escala mundial para otras tecnologías de la comunicación

En nuestros días la red de comunicación más importante es Internet, la cual por el desarrollo y crecimiento exorbitante que ha tenido en las últimas décadas, cuenta con una escasa regulación normativa de protección al usuario. Por ello son frecuentes las violaciones a la esfera privada del individuo, realizadas por medio esta autopista de la información, también llamada “infopista” (Del Peso Navarro y Ramos González, 2002: XXXV). La navegación en la red implica la generación de una serie de datos de carácter personal del usuario y su captación por los diferentes sujetos que intervienen, en mayor o menor medida según sus funciones (Messía de La Cerda Ballesteros, 2004: 101).

No es posible ocultar cómo Internet cambia la cultura de los países, llegando incluso a homogeneizarla, por ello es apremiante una regulación de la materia que sea específica y además eficaz. Tal telaraña universal condensa a la perfección el horizonte digital junto a las últimas tendencias en el tránsito electrónico, erigiéndose de esta forma en la máxima expresión de las nuevas tecnologías (Ballesteros Moffa, 2005: 108-109).

Lo cierto es que hoy en día, la mayoría de los países se preocupan por esto, y han desarrollado diferentes instrumentos como el Convenio 108 del Consejo de Europa, la Directiva 95/46/CE, mismos que paulatinamente se han permeado en las diferentes legislaciones locales. La influencia de dichos ordenamientos se aprecia no solamente en los países de Europa, sino también América latina, tal es el caso de Argentina, México, Colombia, Costa Rica, etc.

México actualmente avanza hacia una cultura de salvaguarda del derecho a la privacidad, mediante una adecuada protección de datos personales, tan es así que pertenece a la Red Iberoamericana de Protección de Datos²³⁵, de la cual se ha

(Muñoz Machado, 2010: 82). Con relación a la sociedad de la información véase también a Comella (2006: 1248-1250).

²³⁵ La cual surge en el año 2003, en la ciudad de la Antigua, en Guatemala, en donde se celebró un Encuentro de Protección de Datos Personales los días 2 a 6 de junio de 2003, del cual surge la Declaración de la Antigua, que consta de nueve puntos, uno de los cuales, el punto número siete es precisamente la creación de la Red Iberoamericana de Protección de Datos. En dicho punto, entre los compromisos que asume, se encuentran el de promover la edición y publicación de documentos de trabajo y de las obras que permitan difundir y dar a conocer los resultados obtenidos en el desarrollo de las actividades de la Red Iberoamericana de Protección de Datos.

desprendido *La Declaración México*²³⁶, en la que el país reconoce la importancia de la protección de datos personales y de la ley que deba regular tal derecho. Y como producto del constante trabajo que ha venido realizando el IFAI, es que hoy día vemos plasmado en la Constitución mexicana los frutos de dicha Declaración, a través del reconocimiento que de tal derecho se precisa los arts. 6, 16 y 73 CPM²³⁷.

3. Definición

Los *datos personales* son cualquier información concerniente a una persona física identificada o identificable. Esta definición es proporcionada por la LAI (art. 3.II) y la LPDP (art. 3.V).

Según la LAI es obligación de los sujetos obligados velar por el cumplimiento del derecho a la protección de datos personales, dichos sujetos lo son (3.XIV LAI): a) El Poder Ejecutivo Federal, la Administración Pública Federal y la Procuraduría General de la República; b) El Poder Legislativo Federal, integrado por la Cámara de Diputados, la Cámara de Senadores, la Comisión Permanente y cualquiera de sus órganos; c) El Poder Judicial de la Federación y el Consejo de la Judicatura Federal; d) Los órganos constitucionales autónomos²³⁸; e) Los tribunales administrativos federales, y f) Cualquier otro órgano federal.

²³⁶ Creada por los miembros de la Red Iberoamericana de Protección de Datos, reunidos en la Ciudad de México y en Huixquilucan (Estado de México), del 2 al 4 de noviembre de 2005, durante la celebración del IV Encuentro Iberoamericano de Protección de Datos Personales. En cuyas conclusiones de 4 de noviembre de 2005, vemos en el inciso 7 lo siguiente: “*así, una ley de protección de datos personales en México debería considerar, los principios de protección de datos personales internacionalmente reconocidos, aplicables tanto a las entidades públicas como privadas; por otro lado, debe adecuarse a las condiciones sociales, políticas y económicas del país, estableciendo al mismo tiempo reglas claras y sencillas que permitan, no sólo su implementación y cumplimiento, sino también un equilibrio entre el flujo de datos personales y su protección. Por último, la ley debe garantizar el ejercicio efectivo del derecho a la protección de datos de las personas y promover una cultura de confianza y de respeto a los derechos humanos, a través de instituciones independientes*”.

²³⁷ Cabe señalar que en el 2010 solo Coahuila, Nuevo León y San Luis Potosí, son los únicos estados de México en cuyas Leyes de Transparencia no aparece la figura de la protección de datos personales. En cuanto a legislaciones locales de protección de datos solo existen en Coahuila, Colima, Distrito Federal, Guanajuato, Morelos, Oaxaca y Tlaxcala (Domínguez González, 2010: 148-161)

²³⁸ El art. 3.IX LAI precisa que los *órganos constitucionales* autónomos son el Instituto Federal Electoral, la Comisión Nacional de los Derechos Humanos, el Banco de México, las

La normativa mexicana de protección de datos personales es global porque ambos ordenamientos combinan la garantía de este derecho fundamental para proteger al individuo de una forma global, es decir, para ejercitarse frente al sector privado (personas físicas o morales de carácter privado) y el público (entes gubernamentales referidos en el art. 3.XIV LAI).

Los *datos sensibles* son un tipo de datos personales especialmente protegidos y son aquellos que afectan a la esfera más íntima de su titular, o cuya utilización indebida pueda dar origen a discriminación o conlleve un riesgo grave para éste. 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 (art. 3VI LPDP)²³⁹.

Existen diferentes categorías de datos, entre otros, los siguientes²⁴⁰:

- Identificación: nombre, domicilio, teléfono, correo electrónico, firma, RFC, CURP, fecha de nacimiento, edad, nacionalidad, estado civil, etc.
- Laborales: puesto, domicilio, correo electrónico y teléfono del trabajo.
- Patrimoniales: información fiscal, historial crediticio, cuentas bancarias, ingresos y egresos, etc.
- Académicos: trayectoria educativa, título, número de cédula, certificados, etc.
- Ideológicos: creencias religiosas, afiliación política y/o sindical, pertenencia a organizaciones de la sociedad civil y/o asociaciones religiosas
- Salud: estado de salud, historial clínico, enfermedades, información relacionada con cuestiones de carácter psicológico y/o psiquiátrico, etc.
- Características personales: tipo de sangre, ADN, huella digital, etc.

universidades y las demás instituciones de educación superior a las que la ley otorgue autonomía y cualquier otro establecido en la CPM.

²³⁹ En cuanto al consentimiento para el tratamiento de datos personales sensibles revisar el art. 9 LPDP.

²⁴⁰ <http://www.ifai.org.mx/Particulares/faq> (consulta: 09/11/2012).

- Características físicas: color de piel, iris y cabellos, señales particulares, etc.
- Vida y hábitos sexuales.
- Origen: étnico y racial.

3. Sujetos

Es de destacar que el derecho a la protección de datos personales en México es amplio, porque protege al individuo de las intervenciones en su vida privada, en lo que hace a los datos en posesión tanto del sector privado, como del público. Por ello, los sujetos obligados se encuentran en la LPDP y en la LAI.

En cuanto al sector privado, la LPDP que es de orden público y de observancia general en toda la República, establece que los sujetos regulados son los particulares sean personas físicas o morales de carácter privado (art. 2 LPDP), con excepción de:

- I. Las sociedades de información crediticia en los supuestos de la Ley para Regular las Sociedades de Información Crediticia y demás disposiciones aplicables, y
- II. 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.

En cuanto al sector público, la LAI que es también de orden público, señala que los sujetos obligados son (art. 3.XIV LAI):

- a) El Poder Ejecutivo Federal, la Administración Pública Federal y la Procuraduría General de la República.
- b) El Poder Legislativo Federal, integrado por la Cámara de Diputados, la Cámara de Senadores, la Comisión Permanente y cualquiera de sus órganos.
- c) El Poder Judicial de la Federación y el Consejo de la Judicatura Federal.
- d) Los órganos constitucionales autónomos.

- e) Los tribunales administrativos federales.
- f) Cualquier otro órgano federal.

4. Objeto

El objeto de la Protección de Datos Personales²⁴¹, se traduce en el espacio de libertad del individuo, entendido de la manera más amplia posible, esto es, como libertad de decisión, de actuación, de ejercicio de derechos fundamentales, etc. (Serrano Pérez, 2003: 53), teniendo la facultad de conocer, acceder, rectificar y cancelar, según el caso, los datos que sobre su persona se contengan en un sistema de datos personales.

El *objeto* de la LPDP es 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 (art. 1 LPDP).

La Ley establece que el *tratamiento* es la obtención, uso, divulgación o almacenamiento de datos personales, por cualquier medio. El uso abarca cualquier acción de acceso, manejo, aprovechamiento, transferencia o disposición de datos personales (art. 3.XVIII LPDP).

De la definición al objeto, se desprende que la Ley regulará el tratamiento de datos personales, para garantizar la privacidad y el derecho a la autodeterminación informativa, y señala que dicho tratamiento deberá ser: legítimo, controlado e informado. Por legítimo se entiende que cumpla con la ley, es decir que se identifique con el principio de licitud. Por controlado, y según la connotación de la palabra, podemos entender que se refiere al tratamiento intervenido, fiscalizado, regulado y/o limitado por la ley. Finalmente, por informado, se desprende que la persona titular de los datos personales deberá

²⁴¹ Llamado también *Hábeas Data* por la doctrina y ordenamientos jurídicos en otros países. En Argentina, dice Carranza Torres (2001: 28) que la Constitución Nacional ha instituido el *hábeas data* como una acción de amparo especial, que permite a toda persona tomar conocimiento de los datos o informaciones a ella referidos, o que lo afecten o puedan afectarla, alterando o restringiendo indebidamente sus derechos, especialmente el de intimidad y a la veracidad de su imagen, y una vez comprobada la inexactitud, falsedad, carácter discriminatorio o lo indebido de la difusión a terceros de los mismos, otorga al afectado la potestad de exigir su supresión, rectificación, modificación, actualización o confidencialidad, según fuere el caso.

tener conocimiento de quién los posee y para qué fin están siendo tratados. Esta regulación al tratamiento de datos personales es con el fin de garantizar, además del derecho a la autodeterminación informativa, la privacidad del individuo.

Es de destacar que la Ley refiere la protección del derecho a la autodeterminación informativa, con lo cual claramente se decanta por denominar así a lo que generalmente se conoce como protección de datos personales. Se ha dicho antes que ambos conceptos refieren la protección del mismo derecho, la diferencia estriba en la denominación que cada país le otorga, y que si recordamos aquella Sentencia del Tribunal Federal alemán, lo designa como derecho a de autodeterminación informativa.

El art. 4 LAI fracción III y VI, en materia autodeterminación informativa, señala como objetivos: garantizar la protección de los datos personales en posesión de los sujetos obligados y contribuir a la democratización de la sociedad mexicana y la plena vigencia del Estado de derecho.

En cuanto al objeto del derecho a la protección de datos en el sector público, se puede ligar esta idea con los deberes de los sujetos obligados, quienes serán responsables de dichos datos y, en relación con estos, deberán (art. 20 LAI):

- I. Adoptar los procedimientos adecuados para recibir y responder las solicitudes de acceso y corrección de datos, así como capacitar a los servidores públicos y dar a conocer información sobre sus políticas en relación con la protección de tales datos²⁴².
- II. Tratar datos personales sólo cuando estos sean adecuados, pertinentes y no excesivos en relación con los propósitos para los cuales se hayan obtenido.
- III. Poner a disposición de los individuos, a partir del momento en el cual se recaben datos personales, el documento en el que se establezcan los propósitos para su tratamiento²⁴³.

²⁴² De conformidad con los lineamientos que al respecto establezca el Instituto o las instancias equivalentes previstas en el art. 61 LAI.

²⁴³ En términos de los lineamientos que establezca el Instituto o la instancia equivalente a que se refiere el art. 61 LAI.

- IV. Procurar que los datos personales sean exactos y actualizados.
- V. Sustituir, rectificar o completar, de oficio, los datos personales que fueren inexactos, ya sea total o parcialmente, o incompletos, en el momento en que tengan conocimiento de esta situación.
- VI. Adoptar las medidas necesarias que garanticen la seguridad de los datos personales y eviten su alteración, pérdida, transmisión y acceso no autorizado.

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 haya mediado el consentimiento expreso, por escrito o por un medio de autenticación similar, de los individuos a que haga referencia la información (art. 21 LAI).

5. Límites

El principio básico para el tratamiento de los datos personales ha de ser el del consentimiento, de forma que, en principio, los datos de personales se deben recabar, tratar o comunicar a terceros con su consentimiento (Piñar Mañas, 2006: 68). Tratándose de datos sensibles, el responsable²⁴⁴ deberá obtener el consentimiento expreso y por escrito del titular para su tratamiento y no se podrán crear bases de datos que contengan datos personales sensibles, sin que se justifique la creación de las mismas para finalidades legítimas.

Los casos en los cuales se podrá prescindir del consentimiento, para su tratamiento, será cuando (art.10 LPDP): a) esté previsto en una Ley; b) los datos figuren en fuentes de acceso público; c) los datos personales se sometan a un procedimiento previo de disociación; d) tenga el propósito de cumplir obligaciones derivadas de una relación jurídica entre el titular y el responsable; e) exista una situación de emergencia que potencialmente pueda dañar a un individuo en su persona o en sus bienes; f) sean indispensables para la atención médica, la prevención, diagnóstico, la prestación de asistencia sanitaria,

²⁴⁴ Persona física o moral de carácter privado que decide sobre el tratamiento de datos personales (art. 3. XIV LPDP).

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 g) se dicte resolución de autoridad competente.

El derecho a la protección de datos personales de ningún modo puede ser de carácter absoluto, sino que debe equilibrarse cuando confluya con otros derechos fundamentales como la información o la tutela judicial efectiva, o bienes constitucionalmente protegidos como la transparencia de los poderes públicos, la protección de la salud, la seguridad nacional u otros intereses públicos regulados legalmente (Piñar Mañas, 2006: 68).

La LPDP señala que los principios y derechos previstos en ella, tendrán como límite en cuanto a su observancia y ejercicio, la protección de la seguridad nacional, el orden, la seguridad y la salud públicos, así como los derechos de terceros (art. 4 LPDP). Por estos conceptos se entiende lo siguiente:

a) Seguridad nacional.

La definición de este concepto es variada y dependiendo del tema que se trate es como cada autor la delimitará, para alguno es un servicio de investigación y asesoría que se proporciona para la toma de decisiones (Calderón Arozqueta y Salgado Garza, 2000: 102), para otro puede estar ligado al bienestar social de la población y desarrollo del país²⁴⁵ (Curzio, 2007: 85), o bien para combatir el terrorismo y fortalecer la democracia (Sepúlveda Amor, 2002: 25-27), entre muchos otros significados y elementos que son proporcionados por la doctrina²⁴⁶.

Para Calderón Arozqueta y Salgado Garza (2000: 102) es un servicio que se dedica a realizar esencialmente una misma actividad, que es la provisión de información auxiliar a la toma de decisiones, a partir de los requerimientos de información solicitados por el cliente, que es el Estado-nación.

²⁴⁵ El autor dice que la definición de la seguridad nacional también está ligada al combate de su nueva amenaza: el narcotráfico.

²⁴⁶ Para mayor abundamiento sobre la evolución del término “seguridad nacional” en México, véase: Curzio (2007: 81-100).

López Chavarría (2005: 298) considera que es el conjunto de acciones gubernamentales tendentes a preservar la tranquilidad del país y sus condiciones de desarrollo, frente a la eventual amenaza o agresiones cometidas por grupos extranjeros o nacionales, que pretenden quebrantar alguna de las decisiones jurídico-políticas fundamentales.

Sepúlveda Amor (2002: 25-27) resalta la importancia de redefinir el concepto de seguridad nacional, de acuerdo a las circunstancias contemporáneas de México y dice que esa seguridad abarca la integridad territorial y la independencia política de México, reafirmando su calidad de Estado soberano, pero que no se limita a ello. Es importante que esa noción de seguridad no tenga una connotación policiaca o militar, sino por el contrario, debe tener alcances eminentemente políticos. El autor refiere que una auténtica seguridad del Estado se convertirá en parte de una seguridad colectiva para la comunidad internacional y que por lo tanto debe comprender una serie de elementos como son: fortalecer las instituciones democráticas, respetar los derechos humanos, reafirmar la existencia de un Estado de Derecho, implantar estrategias de desarrollo económico, combatir el narcotráfico, combatir organizaciones terroristas, combatir a escala internacional el tráfico ilícito de armamentos, combatir la corrupción pública y privada, proteger el medio ambiente, afianzar los mecanismos de solidaridad internacional e integrar programas de salud pública.

Tan difícil es definir la seguridad nacional, que hay que recordar la queja –con plena vigencia hoy- que expresara hace más de tres décadas un congresista norteamericano, Jhon Moss, como presidente de la Comisión que redactó a mediados de los años sesenta la Ley sobre Libertad de Información (*Freedom of Information Act*): “la seguridad nacional es un concepto tan mal definido que aún no he encontrado a nadie capaz de aclararme su significado” (Revenga Sánchez, 1995: 17).

b) Orden público

La Real Academia Española define el orden público como aquella situación y estado de legalidad normal en que las autoridades ejercen sus atribuciones propias y los ciudadanos las respetan y obedecen sin protesta.

Magallón (1965: 662) señala que este término, en general comprende la moral y las buenas costumbres, también dice que a primera vista, la cuestión es muy sencilla y parece fácilmente resumible en un solo concepto; pero que esta aparente sencillez, desaparece en el momento de su aplicación pues tropieza con dificultades muy graves. Y recuerda, entre otras, la definición aportada por Eugenio Audinet cuando define al orden público como “el conjunto de disposiciones legales o de instituciones que en un Estado tienen por objeto regular y defender los derechos de la sociedad y sus intereses generales, considerados en sus diversas relaciones: intereses religiosos, morales, políticos, económicos, de policía y tranquilidad”.

Mansilla y Mejía (2003: 336) reflexiona sobre Savigny cuando dijo que el orden público era un remedio contra la aplicación de la ley extranjera que normalmente debiera aplicarse, este remedio, es una excepción que debe limitarse, y sostenía que: “...cuando la aplicación de la norma extranjera se dirige a un estado de cosas que el legislador considere como destructor del orden social o de la moral, no puede tolerar esta aplicación”. En tal supuesto Savigny considera que el orden público es una excepción, una reserva a la aplicación de la norma extranjera.

Mansilla y Mejía (2003: 337-338) recuerda también lo sostenido por Jitta, quien dijo que el orden público tiene dos sentidos uno amplio y otro restringido: “en el derecho privado nacional está interesado el orden público de todas las instituciones jurídicas que la ley no abandona a la voluntad de los particulares; el estado de las personas es, en este sentido de orden público y por eso los particulares no pueden determinar, mediante un contrato, que su matrimonio haya de ser indisoluble o disoluble bajo condiciones distintas a las condiciones legales...”, “pero en el Derecho Internacional Privado, el principio de orden público no se presenta de ese modo, o con esa amplitud, cuyo efecto sería la paralización de la vida internacional: hay que tomar pues la frase de orden público, dentro de una ciencia en sentido menos amplio, por más que cuando se trata de precisar, sea difícil entenderse. La gran dificultad para llegar a una conclusión, precisa y universalmente aplicable, a la vez, consiste en la necesidad de limitar su aplicación a las leyes extranjeras. Al juez –añade Jitta- no le

corresponde examinar si sus leyes son contrarias al orden público o hasta inmorales, sino que les debe obediencia aunque en su fuero interno las juzgue antisociales e inmorales en el más alto grado. El juez sólo puede criticar las leyes extranjeras, y aún en esta crítica no puede abandonarse libremente a su inspiración”.

El orden público es nacional, lo que significa que cada país tiene su propia concepción del mismo, por lo que puede ocurrir que una institución extranjera quebrante el orden público de un país y no quebrante el de otro. Se puede decir que el concepto que se estudia es temporal y relativa su aplicación, que está a cargo de la autoridad y se determina en cada caso concreto y al aplicarse tiene la naturaleza de una obligación de no hacer (Mansilla Mejía, 2003: 342-350).

El orden público se basa en la idea de la existencia de intereses superiores pertenecientes a la colectividad y a la moral social. En síntesis, el concepto, como muchos otros en el derecho, puede tener amplitud o restrictividad dependiendo de situaciones de carácter político, económico o social vigentes en el tiempo en que se formulan. El orden público interno se puede conceptuar como las disposiciones legislativas resguardantes de los intereses superiores de la colectividad o de la moral social. A su vez el orden público internacional se puede definir como el límite del foro a la aplicación del derecho extranjero, a las leyes, actos y sentencias de otro país. En el orden jurídico interno, el concepto de orden público es un límite a la manifestación de voluntad individual en la forma de disposiciones y convenciones particulares, y en el orden jurídico internacional tiene por objeto limitar la aplicación del derecho extranjero en sus diversas formas (Peña Neira, 1998: 109-111)

De Bartolomé Cenzano (2002: 405-406) señala la necesidad del que el Tribunal Constitucional español interprete el concepto de orden público y en cuanto a la dificultad de definirlo, apunta lo dicho por la STC 33/1982, de 8 de junio (FJ 3): “sin que sea necesario un examen pormenorizado de lo que debe entenderse por Orden Público, es lo cierto que en él pueden incluirse cuestiones como las referentes a la salubridad, (...)”.

c) Seguridad pública

Velar por la Seguridad pública es competencia exclusiva del Estado. Sin que sea necesario un examen pormenorizado de lo que debe entenderse por Orden Público, es lo cierto que en él pueden incluirse cuestiones como las referentes a la salubridad, para limitarse a lo que aquí interesa, que no entran en el concepto de seguridad, la cual se centra en la actividad, dirigida a la protección de personas y bienes (seguridad en sentido estricto) y al mantenimiento de la tranquilidad u orden ciudadano, que son finalidades inseparables y mutuamente condicionadas (De Bartolomé Cenzano, 2002: 413)²⁴⁷. La seguridad pública es una actividad de competencia exclusiva del Estado, dirigida a la protección de personas y bienes y al mantenimiento de la tranquilidad u orden ciudadano (STC 117/1984, FFJJ 1 y 2).

Para González Pérez (2007: 114) el derecho fundamental a la seguridad pública implica una obligación a cargo del Estado, como condición necesaria para el fortalecimiento de la sociedad y uno de los principales elementos para asegurar la calidad de vida de todo ser humano. El autor dice que se puede entender como el servicio que el Estado brinda a la ciudadanía a través de las medidas preventivas o de seguridad, que deben ser oportuna y eficazmente aplicadas por las diversas corporaciones policíacas, a fin de salvaguardar la integridad física, los bienes y los derechos de las personas, así como preservar la libertad, el orden y la paz públicos; y que cuando por alguna circunstancia se rompa ese principio, esto es, que se atente contra alguno de esos derechos, sean los órganos encargados de procurar y administrar la justicia los responsables de lograr, pronta y expeditamente, que se le resarza a dichas personas el pleno goce de los derechos que les fueron afectados, en completa armonía y aplicación de la ley.

El art. 21 CPM establece que la seguridad pública es una función a cargo de la Federación, el Distrito Federal, los Estados y los Municipios, que comprende la prevención de los delitos; la investigación y persecución para hacerla efectiva, así como la sanción de las infracciones administrativas, en los

²⁴⁷ Afirmar esto no supone negar que una crisis sanitaria pueda amenazar la seguridad pública y justificar, en consecuencia, una intervención de las autoridades a las que corresponda su custodia. Incluso es de recordar que crisis sanitarias tales como epidemias y situaciones de contaminación graves pueden motivar la declaración del Estado de Alarma (España LO 4/1981, de 1 de junio, art. 4.b) (De Bartolomé Cenzano, 2002: 413).

términos de la ley, en las respectivas competencias que esta Constitución señala. La actuación de las instituciones de seguridad pública se regirá por los principios de legalidad, objetividad, eficiencia, profesionalismo, honradez y respeto a los derechos humanos reconocidos en esta Constitución. Las instituciones de seguridad pública serán de carácter civil, disciplinado y profesional. El Ministerio Público y las instituciones policiales de los tres órdenes de gobierno deberán coordinarse entre sí para cumplir los objetivos de la seguridad pública y conformarán el Sistema Nacional de Seguridad Pública, que estará sujeto a las siguientes bases mínimas:

- a) La regulación de la selección de ingreso, formación, permanencia, evaluación, reconocimiento y certificación de los integrantes de las instituciones de seguridad pública. La operación y desarrollo de estas acciones será competencia de la Federación, el Distrito Federal, los Estados y los municipios en el ámbito de sus respectivas atribuciones.
- b) El establecimiento de las bases de datos criminalísticos y de personal para las instituciones de seguridad pública. Ninguna persona podrá ingresar a las instituciones de seguridad pública si no ha sido debidamente certificado y registrado en el sistema.
- c) La formulación de políticas públicas tendientes a prevenir la comisión de delitos.
- d) Se determinará la participación de la comunidad que coadyuvará, entre otros, en los procesos de evaluación de las políticas de prevención del delito así como de las instituciones de seguridad pública.
- e) Los fondos de ayuda federal para la seguridad pública, a nivel nacional serán aportados

d) Salud pública

La salud pública es la actividad encaminada a mejorar la salud de la población, que es lo que preocupa dentro de este concepto y no la disciplina de la medicina como tal. Las acciones de salud pública no son sólo responsabilidad del

Estado sino de toda la sociedad, lo cual implica que entes privados tienen igualmente importantes responsabilidades y actividades que cumplir en este ámbito (Blanco Restrepo y Maya Mejía: 2005:5-7).

Las Funciones Esenciales de Salud Pública (FESP) describen el espectro de competencias y acciones necesarias por parte de los sistemas de salud para alcanzar el objetivo central de la salud pública, que es el mejorar la salud de las poblaciones. La Organización Panamericana de la Salud (OPS) por medio de la Iniciativa “La Salud Pública en las Américas”, definió once FESP y desarrolló un instrumento para medir su desempeño, lo que permite a los países realizar una auto-evaluación de sus capacidades para ejercer la salud pública²⁴⁸, que son:

1. El monitoreo, la evaluación y el análisis del estado de salud de la población.
2. La vigilancia, la investigación y el control de los riesgos y las amenazas para la salud pública.
3. La promoción de la salud.
4. El aseguramiento de la participación social en la salud.
5. La formulación de las políticas y la capacidad institucional de reglamentación y cumplimiento en la salud pública.
6. El fortalecimiento de la capacidad institucional de planificación y el manejo en la salud pública.
7. La evaluación y la promoción del acceso equitativo a los servicios de salud necesarios.
8. La capacitación y desarrollo de los recursos humanos.
9. La seguridad de la calidad en los servicios de salud.
10. La investigación en la salud pública.

²⁴⁸ Los Ministerios o Secretarías de Salud pueden a través de este instrumento identificar, no solo los factores críticos que deben tenerse en cuenta para desarrollar planes o estrategias de fortalecimiento de la infraestructura institucional de la salud pública sino también los mecanismos de gestión y recursos materiales necesarios para que la Autoridad Sanitaria Nacional (ASN), en sus diferentes niveles de intervención, pueda ejercer de manera óptima las funciones que le competen. Fuente: <http://www.paho.org/spanish/dpm/shd/hp/FESP.htm> (Consulta: 09/11/2012).

11. La reducción de la repercusión de las emergencias y los desastres en la salud pública.

En lo que hace al tema de la salud pública en el ámbito internacional, en España y acorde con lo dispuesto por el Código Mundial Antidopaje, la LO 7/2006, de protección de la salud y de lucha contra el dopaje y el deporte, en su exposición de motivos refiere que para intentar asegurar el cumplimiento de ciertas medidas²⁴⁹ se arbitra un ámbito de tutela penal de la salud pública en actividades relacionadas con el dopaje en el deporte. Se introduce un nuevo artículo 361 bis en el Código Penal, cuya finalidad es castigar el entorno del deportista y preservar la salud pública, gravemente amenazada por la comercialización y dispensación sin control de productos carentes de garantía alguna y dañinos para la salud.

El art. 14 del referido Código Mundial, prevé que a la hora de cumplir las obligaciones establecidas en este ordenamiento, las organizaciones antidopaje podrán obtener, almacenar, procesar, o divulgar datos personales de los deportistas y terceras partes. Cada organización antidopaje garantizará el cumplimiento de la legislación aplicable sobre confidencialidad y protección de datos con respecto al manejo de dicha información, así como la norma internacional para la protección de la intimidad que adopte la Agencia Mundial Antidopaje para garantizar que los deportistas y quienes no lo son estén plenamente informados y, en caso necesario, accedan a que se utilicen sus datos personales en relación con actividades antidopaje iniciadas como consecuencia de lo establecido en dicho Código. Al respecto, la interrogante que se puede plantear es si esto evolucionará a un banco de datos internacional especializado con tales datos sensibles, bajo la justificación de la lucha contra el dopaje (Marafioti, 2010: 85).

²⁴⁹ El título segundo de la Ley se refiere a aspectos genéricos de control del dopaje en el deporte, ya sea éste el de competición o el de mera recreación. Se incluyen un conjunto de medidas, como son la supervisión y revisión del contenido de los botiquines médicos en las competiciones deportivas, la determinación del seguimiento de los medicamentos y productos susceptibles de causar dopaje en el deporte, con el fin de conocer en que momento se altera la cadena de distribución comercial, poniendo los medios para impedir que esos mismos productos o falsificaciones de ellos afloren al mercado en condiciones distintas a las que establece la normativa vigente para su dispensación, o la fijación de estrictas condiciones de comercialización y de control de los productos que pueden causar dopaje en el deporte

En México el dopaje de los deportistas no se encuentra previsto en el Código Penal Federal, únicamente se considera una infracción administrativa el resultado positivo del antidopaje (art. 115 de la Ley General de cultura física y deporte).

e) **Derechos de terceros**

Para que en una sociedad democrática rija el Estado de Derecho y la confianza de la sociedad en el mismo, se requiere de una apropiada rendición de cuentas, la que no se puede comprobar sin una cultura de transparencia y acceso a la información.

Y en cuanto a este punto hemos de decir que la protección de datos personales nunca ha de ser en perjuicio de lo que engloba el ejercicio del derecho al acceso a la información pública y transparencia gubernamental.

6. Autoridades

El Instituto (conocido como IFAI), que comenzó a operar oficialmente en junio de 2003, es el órgano regulador de la materia y es definido de diversa forma, según la Ley de que se trate, ya que vela por el derecho a la información y el de protección de datos personales. Este es garante del derecho a la protección de datos personales en posesión de particulares, a partir de la publicación de la LPDP en 2010²⁵⁰.

El Instituto de Acceso a la Información Pública y Protección de Datos, específicamente para efectos de la LPDP, tendrá por objeto 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 Ley y que deriven de la misma; en particular aquellas relacionadas con el cumplimiento de obligaciones por parte de los sujetos regulados (art. 38 LPDP), es decir, los particulares que sean personas físicas o morales de carácter privado.

²⁵⁰ Por ello cambió de nombre pasando de Instituto Federal de Acceso a la Información a Instituto Federal de Acceso a la Información Pública y Protección de Datos

Por otro lado, la LAI establece que el Instituto es un órgano de la Administración Pública Federal, con autonomía operativa, presupuestaria y de decisión, encargado de promover y difundir el ejercicio del derecho a la información; resolver sobre la negativa a las solicitudes de acceso a la información y proteger los datos personales en poder de las dependencias y entidades (art. 33 LAI).

El IFAI está integrado por cinco comisionados, cuyo nombramiento corresponde al Poder Ejecutivo Federal²⁵¹ y duraran en su encargo siete años sin posibilidad de reelección. El Instituto estará presidido por un Comisionado, quien tendrá la representación legal del mismo, dicho encargo tendrá una duración de dos años, renovable por una ocasión y será elegido por los comisionados (arts. 35 y 36 LAI).

6.1 El Instituto Federal de Acceso a la Información y Protección de datos personales

El Instituto es la Autoridad garante del derecho a la protección de datos personales, teniendo por objeto difundir el conocimiento de este en la sociedad mexicana, promover su ejercicio y vigilar por la debida observancia de la LPDP. Tiene además las siguientes atribuciones (art. 39 LPDP):

1. Vigilar y verificar el cumplimiento de las disposiciones contenidas en esta Ley, en el ámbito de su competencia, con las excepciones previstas por la legislación.
2. Interpretar en el ámbito administrativo la LPDP.
3. Proporcionar apoyo técnico a los responsables que lo soliciten, para el cumplimiento de las obligaciones establecidas en la Ley.
4. Emitir los criterios y recomendaciones, de conformidad con las disposiciones aplicables de esta Ley, para efectos de su funcionamiento y operación.

²⁵¹ La Cámara de Senadores puede objetar dichos nombramientos por mayoría, y cuando se encuentre en receso lo podrá hacer la Comisión Permanente

5. Divulgar estándares y mejores prácticas internacionales en materia de seguridad de la información, en atención a la naturaleza de los datos; las finalidades del tratamiento, y las capacidades técnicas y económicas del responsable.
6. Conocer y resolver los procedimientos de protección de derechos y de verificación señalados en esta Ley e imponer las sanciones según corresponda.
7. Cooperar con otras autoridades de supervisión y organismos nacionales e internacionales, a efecto de coadyuvar en materia de protección de datos.
8. Rendir al Congreso de la Unión un informe anual de sus actividades.
9. Acudir a foros internacionales en el ámbito de la presente Ley.
10. Elaborar estudios de impacto sobre la privacidad previos a la puesta en práctica de una nueva modalidad de tratamiento de datos personales o a la realización de modificaciones sustanciales en tratamientos ya existentes.
11. Desarrollar, fomentar y difundir análisis, estudios e investigaciones en materia de protección de datos personales en Posesión de los Particulares y brindar capacitación a los sujetos obligados.
12. Las demás que le confieran esta Ley y demás ordenamientos aplicables.

Asimismo, el Instituto será competente para conocer y substanciar, conforme a la Ley y Reglamento de la materia, los siguientes procedimientos:

- a) Protección de derechos (arts. 45 a 58 LPDP y arts. 113 a 127 RLPDP).
- b) Verificación (arts. 59 a 60 LPDP y arts. 128 a 139 RLPDP).
- c) Imposición de sanciones (arts. 61 a 62 LPDP y arts. 140 a 144 RLPDP).

6.2 Autoridades reguladoras

En lo que hace a este apartado, la Ley precisa que a fin de garantizar la protección de este derecho, en coadyuvancia con el Instituto, habrá distintos

actores que podrán emitir la regulación que corresponda para dar cumplimiento a la normativa y son:

a) Las Dependencias

La LPDP será el marco normativo que las dependencias deberán observar en el ámbito de sus propias atribuciones, para la emisión de la regulación que corresponda. Dichas dependencias son: Secretaría de Gobernación, Secretaría de Relaciones Exteriores, Secretaría de la Defensa Nacional, Secretaría de Marina, Secretaría de Seguridad Pública, Secretaría de Hacienda y Crédito Público, Secretaría de Desarrollo Social, Secretaría de Medio Ambiente y Recursos Naturales, Secretaría de Energía, Secretaría de Economía, Secretaría de Agricultura, Ganadería, Desarrollo Rural, Pesca y Alimentación, Secretaría de Comunicaciones y Transportes, Secretaría de la Función Pública, Secretaría de Educación Pública, Secretaría de Salud, Secretaría del Trabajo y Previsión Social, Secretaría de la Reforma Agraria, Secretaría de Turismo²⁵².

b) Secretaría de Economía

La Secretaría de Economía (en adelante la Secretaría), para efectos de la Ley, tendrá como función difundir el conocimiento de las obligaciones en torno a la protección de datos personales entre la iniciativa privada nacional e internacional con actividad comercial en territorio mexicano; promoverá las mejores prácticas comerciales en torno a la protección de los datos personales como insumo de la economía digital, y el desarrollo económico nacional en su conjunto (art. 41 LPDP). En lo referente a las bases de datos de comercio, la regulación que emita la Secretaría, únicamente será aplicable a aquellas bases de datos automatizadas o que formen parte de un proceso de automatización (art. 42 LPDP).

La Secretaría tiene las siguientes atribuciones (art. 43 LPDP):

1. Difundir el conocimiento respecto a la protección de datos personales en el ámbito comercial.

²⁵² Art. 40 LPDP, en relación con el art. 26 de la Ley Orgánica de la Administración Pública Federal (DOF 14/06/2012).

2. Fomentar las buenas prácticas comerciales en materia de protección de datos personales.
3. Emitir los lineamientos correspondientes para el contenido y alcances de los avisos de privacidad en coadyuvancia con el Instituto, a que se refiere la Ley.
4. Emitir, en el ámbito de su competencia, las disposiciones administrativas de carácter general a que se refiere el art. 40 LPDP, en coadyuvancia con el Instituto.
5. Fijar los parámetros necesarios para el correcto desarrollo de los mecanismos y medidas de autorregulación a que se refiere el art. 44 LPDP, incluido la promoción de Normas Mexicanas o Normas Oficiales Mexicanas, en coadyuvancia con el Instituto.
6. Llevar a cabo los registros de consumidores en materia de datos personales y verificar su funcionamiento.
7. Celebrar convenios con cámaras de comercio, asociaciones y organismos empresariales en lo general, en materia de protección de datos personales.
8. Diseñar e instrumentar políticas y coordinar la elaboración de estudios para la modernización y operación eficiente del comercio electrónico, así como para promover el desarrollo de la economía digital y las tecnologías de la información en materia de protección de datos personales.
9. Acudir a foros comerciales nacionales e internacionales en materia de protección de datos personales, o en aquellos eventos de naturaleza comercial.
10. Apoyar la realización de eventos, que contribuyan a la difusión de la protección de los datos personales.

En este sentido, la Secretaría de Economía en conjunto con el IFAI emitió en junio de 2011 la Guía práctica para generar el aviso de privacidad, en la que orienta a los responsables del tratamiento de datos personales en la elaboración,

diseño y difusión de aviso de privacidad. Esta guía es muy completa y ejemplifica los requerimientos de la Ley para el citado aviso, sin embargo, el aviso se convierte, por su longitud cuando es completo y no simplificado, en algo muy parecido a un contrato adicional que el titular de los datos debe de consentir, situación que es poco práctica a efectos de difusión y concientización²⁵³.

c) Personas físicas o morales

Las personas físicas o morales podrán convenir entre ellas o con organizaciones civiles o gubernamentales, nacionales o extranjeras, esquemas de autorregulación vinculante en la materia, que complementen lo dispuesto por la Ley. Dichos esquemas deberán contener mecanismos para medir su eficacia en la protección de los datos, consecuencias y medidas correctivas eficaces en caso de incumplimiento (art. 44 LPDP).

Los esquemas de autorregulación podrán traducirse en códigos deontológicos o de buena práctica profesional, sellos de confianza u otros mecanismos y contendrán reglas o estándares específicos que permitan armonizar los tratamientos de datos efectuados por los adheridos y facilitar el ejercicio de los derechos de los titulares. Dichos mecanismos serán notificados de manera simultánea a las autoridades sectoriales correspondientes y al Instituto.

Es importante la mención de estos esquemas de autorregulación, ya que facilitan la labor del Instituto, mediante la colaboración en lo que hace a la difusión del derecho y cumplimiento de la Ley. Sin embargo, y dado que se está en un proceso de implementación de la nueva normativa, es conveniente que el Instituto aclare cuáles serían dichos esquemas. En lo que concierne a los sellos de confianza, es probable que se refiera a controles de calidad como el ISO (*International Organization for Standardization*) o Europrise (*European Privacy Seal*) que existen actualmente a nivel internacional y regional, respectivamente.

²⁵³ Se convierte en algo difícil de leer y comprender por el ciudadano, además que por su longitud propicia la pereza en la lectura. Particularmente, considero que un aviso sencillo, corto y conciso, con los datos más importantes, es de más ayuda al momento de comunicar al usuario el tratamiento que se dará a su información personal y las acciones que puede ejercitar.

En este orden de ideas, sería conveniente crear un mecanismo igual a nivel nacional, regulado por el Instituto y cuya licencia se otorgue a profesionales técnico-especializados en la materia. Así, se promovería el interés de la comunidad jurídica en esta área para lograr avances significativos en el cumplimiento de la LPDP, además se incentivaría la cooperación y participación internacional en este campo.

7. Principios de la protección de datos personales en posesión del sector público

La descripción de estos principios atiende al tratamiento de los datos y se encuentran en los Lineamientos y no un Reglamento como es el caso de la LPDP. Es de precisar la importancia de homogenizar la regulación de este tema en el sector público y privado a fin de clarificar el tema. La lista de los principios en uno y otro, no se comparten en su totalidad en lo que hace a la denominación y el contenido; por ejemplo, los que no se aprecian claramente en la regulación del sector público, y si en el privado, son los de *finalidad, lealtad, proporcionalidad y responsabilidad*; pero que se ven en el conjunto de la definición del principio de calidad como: *exacto (lealtad), adecuado (Responsabilidad), pertinente (Finalidad y responsabilidad) y no excesivo (Proporcionalidad, lealtad y finalidad)*. Por su parte, el de Seguridad que se encuentra en este apartado y cuya nomenclatura cambia en el de particulares por el de Responsabilidad, no termina por precisar el aspecto del deber de secreto.

El documento sobre los Lineamientos de Protección de Datos Personales²⁵⁴, establece que en el tratamiento de datos personales, las dependencias y entidades²⁵⁵ deberán observar los principios de: licitud, calidad, acceso y corrección, de información, seguridad, custodia y consentimiento para

²⁵⁴ Publicados en el DOF el viernes 30 de septiembre de 2005.

²⁵⁵ El art. 3.IV LAI las define como aquellas señaladas en la Ley Orgánica de la Administración Pública Federal, incluidas la Presidencia de la República, los órganos administrativos desconcentrados, así como la Procuraduría General de la República.

su transmisión²⁵⁶. Dicho instrumento, define cada uno de ellos de la forma que se verá en este epígrafe.

7.1 Licitud

La posesión de sistemas de datos personales deberá obedecer exclusivamente a las atribuciones legales o reglamentarias de cada dependencia o entidad y deberán obtenerse a través de los medios previstos en dichas disposiciones.

Los datos personales deberán tratarse únicamente para la finalidad para la cual fueron obtenidos. Dicha finalidad debe ser determinada y legítima (Lineamiento sexto).

7.2 Calidad de los datos

El tratamiento de datos personales deberá ser exacto, adecuado, pertinente y no excesivo, respecto de las atribuciones legales de la dependencia o entidad que los posea. Dichas características son explicadas por los propios Lineamientos de Protección de Datos Personales de la siguiente forma²⁵⁷:

- a) Exacto: cuando los datos personales se mantienen actualizados de manera tal que no altere la veracidad de la información y que traiga como consecuencia que el titular de los datos se vea afectado por dicha situación.
- b) Adecuado: cuando se observen las medidas de seguridad aplicables.
- c) Pertinente: cuando es realizado por el personal autorizado para el cumplimiento de las atribuciones de las dependencias y entidades que los hayan recabado.
- d) No excesivo: cuando la información solicitada al Titular de los datos es estrictamente la necesaria para cumplir con los fines para los cuales se hubieran recabado.

²⁵⁶ Capítulo II, sobre los principios rectores de la protección de datos personales. Quinto a duodécimo de los Lineamientos de Protección de Datos Personales.

²⁵⁷ Lineamientos séptimo y decimotercero de Protección de Datos Personales.

7.2.1 Acceso y corrección

Los sistemas de datos personales deberán almacenarse de forma tal que permitan el ejercicio de los derechos de acceso y corrección previstos por la Ley, el Reglamento y los Lineamientos emitidos por el Instituto.

El lineamiento decimocuarto, sobre la corrección, establece que en caso de que los responsables, encargados o usuarios detecten que hay datos personales inexactos, deberán de oficio, actualizarlos en el momento en que tengan conocimiento de la inexactitud de los mismos, siempre que posean los documentos que justifiquen la actualización.

7.2.2 De Información

Se deberá hacer del conocimiento del titular de los datos, al momento de recabarlos y de forma escrita, el fundamento y motivo de ello, así como los propósitos para los cuales se tratarán dichos datos.

El lineamiento decimoséptimo, sobre la información al titular de los datos, señala que en el momento en que se recaben datos personales, la dependencia o entidad deberá hacer del conocimiento al titular de los datos tanto en los formatos físicos como en los electrónicos utilizados para ese fin, lo siguiente²⁵⁸:

- a) La mención de que los datos recabados serán protegidos en términos de lo dispuesto por la Ley.
- b) El fundamento legal para ello.
- c) La finalidad del Sistema de datos personales.

7.2.3 Seguridad

Se deberán adoptar las medidas necesarias para garantizar la integridad, confiabilidad, confidencialidad y disponibilidad de los datos personales mediante acciones que eviten su alteración, pérdida, transmisión y acceso no autorizado.

²⁵⁸ El lineamiento decimoctavo anota un modelo de leyenda para informar al titular de los datos.

El lineamiento decimosexto, sobre las condiciones técnicas de seguridad, refiere que los datos sólo podrán ser tratados en sistemas de datos personales que reúnan las condiciones de seguridad establecidas en los Lineamientos de Protección de Datos Personales emitidos por el IFAI.

El lineamiento vigésimo primero, sobre el tratamiento de datos por terceros, establece que cuando se contrate a terceros para que realicen el tratamiento de datos personales, deberá estipularse en el contrato respectivo, la implementación de medidas de seguridad y custodia previstas en los Lineamientos de Protección de Datos Personales, en la normatividad aplicable a las dependencias y entidades contratantes, así como la imposición de penas convencionales por su incumplimiento.

7.2.4 Custodia y cuidado de la información

Los datos personales serán debidamente custodiados y los responsables, encargados y usuarios deberán garantizar el manejo cuidadoso en su tratamiento.

El lineamiento decimoquinto, sobre la conservación de los datos, establece que aquellos que hayan sido objeto de tratamiento y no contengan valores históricos, científicos, estadísticos o contables, deberán ser dados de baja por las dependencias y entidades²⁵⁹.

7.2.5 Consentimiento para la transmisión

Toda transmisión de datos personales deberá contar con el consentimiento del Titular de los datos, mismo que deberá otorgarse en forma libre, expresa e informada.

²⁵⁹ Este mismo lineamiento, establece que por otro lado, los que contengan dichos valores serán objeto de transferencias secundarias, de conformidad con lo establecido por los catálogos de disposición documental a que se refieren los Lineamientos Generales para la organización y conservación de archivos de las Dependencias y entidades de la Administración Pública Federal, teniendo en cuenta los siguientes plazos: a) el que se haya establecido en el formato físico o electrónico por el cual se recabaron; b) el establecido por las disposiciones aplicables; c) el establecido en los convenios formalizados entre una persona y la dependencia o entidad, y c) el señalado en los casos de transmisión.

La excepción a lo anterior es que las dependencias y entidades podrán transmitir datos personales sin el consentimiento del titular de los datos, cuando²⁶⁰:

- a) Estos sean necesarios por razones estadísticas, científicas o de interés general previstas en la ley, previo procedimiento por el cual no puedan asociarse los datos personales con el individuo a quien se refieran.
- b) Se transmitan entre sujetos obligados o entre dependencias y entidades, siempre y cuando los datos se utilicen para el ejercicio de facultades propias de los mismos.
- c) Exista una orden judicial.
- d) A terceros se contrate la prestación de un servicio que requiera el tratamiento de datos personales. Dichos terceros no podrán utilizar los datos personales para propósitos distintos a aquellos para los cuales se les hubieren transmitido.
- e) Y los demás casos que establezcan las leyes.

El lineamiento vigésimo tercero, sobre la transmisión con el consentimiento del titular de los datos, establece que para los efectos del art. 21 LAI²⁶¹, y en los casos no previstos por el art. 22 LAI²⁶², las dependencias y entidades sólo podrán transmitir datos personales cuando: a) así lo prevea de

²⁶⁰ Lineamientos de Protección de Datos Personales (lineamiento vigésimo segundo) y art. 22 LAI.

²⁶¹ Artículo 21. 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 haya mediado el consentimiento expreso, por escrito o por un medio de autenticación similar, de los individuos a que haga referencia la información.

²⁶² Artículo 22. No se requerirá el consentimiento de los individuos para proporcionar los datos personales en los siguientes casos: I. (Se deroga) *Fracción derogada DOF 11-05-2004*; II. 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; III. Cuando se transmitan entre sujetos obligados o entre dependencias y entidades, siempre y cuando los datos se utilicen para el ejercicio de facultades propias de los mismos; IV. Cuando exista una orden judicial; V. A terceros cuando se contrate la prestación de un servicio que requiera el tratamiento de datos personales. Dichos terceros no podrán utilizar los datos personales para propósitos distintos a aquellos para los cuales se les hubieren transmitido, y VI. En los demás casos que establezcan las leyes.

manera expresa una disposición legal, y b) medie el consentimiento expreso de los titulares.

El lineamiento vigésimo cuarto, sobre el consentimiento, señala que para la transmisión de los datos, el consentimiento del Titular de los mismos deberá otorgarse por escrito incluyendo la firma autógrafa y la copia de identificación oficial, o bien a través de un medio de autenticación. En su caso, las dependencias y entidades deberán cumplir con las disposiciones aplicables en materia de certificados digitales y/o firmas electrónicas. El servidor público encargado de recabar el consentimiento del Titular de los datos para la transmisión, la información suficiente acerca de las implicaciones de otorgar, de ser el caso, su consentimiento.

8. Principios de la protección de datos personales en posesión de particulares

Estos principios se encuentran en la Ley Federal de Protección de Datos Personales en posesión de los particulares, así como en su reglamento respectivo; a diferencia de los que priman en el sector público que se encuentran en los Lineamientos de Protección de Datos Personales, expedidos por el IFAI.

Los responsables en el tratamiento de datos personales, deberán observar los principios de licitud, consentimiento, información, calidad, finalidad, lealtad, proporcionalidad y responsabilidad (art. 6 LPDP y art. 9 RLPDP)

8.1 Licitud

Se refiere al compromiso que deben asumir los entes privados (personas físicas o morales) para tratar la información de un particular cuando este solicita la prestación de un bien o servicio, respetando en todo momento la confianza que les ha sido depositada para el buen uso que darán de esa información²⁶³.

El art. 7 LPDP establece que los datos personales deberán recabarse y tratarse de manera lícita conforme a las disposiciones establecidas por la LPDP y demás normativa aplicable. La obtención de dicha información no debe hacerse a través de medios engañosos o fraudulentos. Por su parte, el Reglamento a la Ley

²⁶³ <http://www.ifai.org.mx/Particulares/faq> (consulta: 09/11/2012).

agrega que dicho tratamiento deberá hacerse atendiendo a la legislación mexicana y el derecho internacional (art. 10 RLPDP). Esta mención al derecho internacional es significativa, no sólo por los instrumentos internacionales regionales que existen en Europa, sino además por que existe la tendencia actual a la estandarización de la normativa del derecho a la protección de datos personales, y no sería raro que en el futuro puedan aparecer.

En todo tratamiento de datos personales, se presume que existe la *expectativa razonable de privacidad*, que es la confianza que deposita cualquier persona en otra al proporcionar los datos personales esperando que sean tratados conforme a lo que acordaron en los términos previstos en la Ley.

8.2 Consentimiento

Este principio hace posible que el particular pueda decidir de manera informada, libre, inequívoca y específica si quiere compartir información con otras personas. Para las empresas que posean dicha información personal, implica el deber de solicitar la autorización por parte del titular de los datos para que puedan ser tratados, especialmente cuando se trata de datos sensibles que afectan la esfera más íntima de la persona. La ley exige a las empresas solicitar el consentimiento de manera expresa y por escrito. Adicionalmente deberán implementar medidas de seguridad muy estrictas que eviten quebrantar la confidencialidad, integridad y disponibilidad de los datos²⁶⁴.

El consentimiento es la manifestación de la voluntad del titular de los datos mediante la cual se efectúa el tratamiento de los mismos (art. 3.IV LPDP). El art. 8 LPDP refiere que todo tratamiento de datos personales estará sujeto al consentimiento de su titular, salvo las excepciones previstas por la Ley, las cuales se verán con posterioridad. Por su parte, el reglamento establece que la solicitud del consentimiento deberá ir referida a una finalidad o finalidades determinadas, previstas en el aviso de privacidad (art. 11 RLPDP).

²⁶⁴ <http://www.ifai.org.mx/Particulares/faq> (consulta: 09/11/2012).

8.2.1 Características del consentimiento

El Reglamento establece que el consentimiento, tácito o expreso, habrá de reunir tres características que son (art. 12 RLPDP):

1. Libre: sin que medie error, mala fe, violencia o dolo, que puedan afectar la manifestación de voluntad del titular.
2. Específica: referida a una o varias finalidades determinadas que justifiquen el tratamiento.
3. Informada: que el titular tenga conocimiento del aviso de privacidad previo al tratamiento a que serán sometidos sus datos personales y las consecuencias de otorgar su consentimiento.

8.2.2 Tipos de consentimiento

El art. 8 LPDP, como innovación a otros ordenamientos, el mexicano acepta y distingue dos tipos de consentimiento, que son:

1. El *consentimiento expreso*: aquel cuya voluntad se manifiesta verbalmente²⁶⁵, por escrito²⁶⁶, por medios electrónicos, ópticos o por cualquier otra tecnología, o por signos inequívocos. El art. 15 RLPDP dice que se obtendrá cuando: a) lo exija una ley o reglamento; b) se trate de datos financieros o patrimoniales; c) se trate de datos sensibles; d) lo solicite el responsable para acreditar el mismo, o e) lo acuerden así el titular y el responsable.
2. El *consentimiento tácito*: aquel que se da cuando habiéndose puesto a su disposición el aviso de privacidad, el titular no manifiesta su oposición. Este tipo de consentimiento será válido como regla general, salvo que la Ley exija el consentimiento expreso (arts. 13 y 14 RLPDP). Esta tipología es una novedad mexicana, y el reglamento no es claro en el mecanismo

²⁶⁵ Se entenderá así cuando el titular lo externa oralmente de manera presencial o mediante el uso de cualquier tecnología que permita la interlocución oral (art. 18 RLPDP).

²⁶⁶ Se entenderá así cuando el titular lo externe mediante un documento con su firma autógrafa, huella dactilar o cualquier otro mecanismo autorizado por la normativa aplicable. Tratándose del entorno digital, podrán utilizarse firma electrónica o cualquier mecanismo o procedimiento que al efecto se establezca y permita identificar al titular y recabar su consentimiento (art. 19 RLPDP)

que se habrá de seguir en el propio aviso de privacidad, para que titular manifieste su negativa al tratamiento.

8.2.3 Datos financieros y patrimoniales

La Ley establece que para los datos financieros o patrimoniales se requerirá del consentimiento expreso de su titular, salvo las excepciones señaladas en el art. 10 y 37 LPDP, que son las excepciones al consentimiento que se verán más adelante.

8.2.4 Datos sensibles

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 (art. 9 LPDP).

Asimismo la Ley establece que no podrán crearse bases de datos que contengan datos personales sensibles, sin que se justifique la creación de las mismas para finalidades legítimas, concretas y acordes con las actividades o fines explícitos que persigue el sujeto regulado.

Legalmente, sólo se podrán crear bases de datos con contenido sensible cuando (art. 56 RLPDP): a) obedezcan a un mandato legal; b) se justifique en términos del art. 4 LPDP²⁶⁷; o 3) el responsable lo requiera para finalidades legítimas, concretas y acordes con las actividades o fines explícitos que persiga.

En lo que hace al supuesto número tres, tenemos las bases de datos médicas de hospitales o clínicas, así como de congregaciones religiosas, sindicatos, Asociaciones, ONG's, etc.

La Ley mexicana, comparada con la española, no contempla el registro de Ficheros ante la Autoridad reguladora, lo que puede representar riesgos para la población por parte del Responsable o encargado. Si quien recopila la

²⁶⁷ Art. 4 LPDP. Los principios y derechos previstos en esta Ley, tendrán como límite en cuanto a su observancia y ejercicio, la protección de la seguridad nacional, el orden, la seguridad y la salud públicos, así como los derechos de terceros.

información no tiene clara la Ley, ni los datos que puede tratar –lo que no es raro cuando se está en fase de implementación de una nueva normativa-, existe el peligro de crear ficheros y tratar información excesiva por no estar correctamente asesorados. La inscripción de ficheros es una medida que, en este caso, podría ser preventiva para no almacenar datos personales en una base de datos sensible, que con posterioridad resultase ilegal. Esto aunado a que las medidas de seguridad previstas por el Reglamento pueden dar lugar a dudas, para lo cual sería importante un Reglamento de seguridad.

Ligando el consentimiento en datos sensibles con el principio de proporcionalidad, hay que recordar que la Ley establece que el tratamiento de datos personales será el que resulte necesario, adecuado y relevante en relación con las finalidades previstas en el aviso de privacidad. En particular para datos personales sensibles, el responsable deberá realizar esfuerzos razonables para limitar el periodo de tratamiento de los mismos a efecto de que sea el mínimo indispensable (art. 13 LPDP).

8.2.5 Excepciones al consentimiento

No será necesario el consentimiento para el tratamiento de los datos personales cuando (art. 10 LPDP y art. 17 RLPDP):

1. Esté previsto en una Ley.
2. Los datos figuren en fuentes de acceso público.
3. Los datos personales se sometan a un procedimiento previo de disociación.
4. Tenga el propósito de cumplir obligaciones derivadas de una relación jurídica entre el titular y el responsable.
5. Exista una situación de emergencia que potencialmente pueda dañar a un individuo en su persona o en sus bienes.
6. 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.

7. Se dicte resolución de autoridad competente.

Las transferencias nacionales o internacionales de datos podrán llevarse a cabo sin el consentimiento del titular cuando se de alguno de los siguientes supuestos (art. 37 LPDP):

1. Cuando la transferencia esté prevista en una Ley o Tratado en los que México sea parte.
2. 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.
3. 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.
4. Cuando la transferencia sea necesaria por virtud de un contrato celebrado o por celebrar en interés del titular, por el responsable y un tercero.
5. Cuando la transferencia sea necesaria o legalmente exigida para la salvaguarda de un interés público, o para la procuración o administración de justicia.
6. Cuando la transferencia sea precisa para el reconocimiento, ejercicio o defensa de un derecho en un proceso judicial.
7. Cuando la transferencia sea precisa para el mantenimiento o cumplimiento de una relación jurídica entre el responsable y el titular.

8.3 Información

Se refiere a la potestad que te otorga la Ley de conocer previamente las características esenciales del tratamiento a que serán sometidos los datos personales que el particular proporciona a un ente privado o empresa. Dicha comunicación deberá ser en un lenguaje comprensible para todas las personas. Las empresas y las personas físicas, que tratan esta información, deben dar a conocer esas características a través del "aviso de privacidad"²⁶⁸.

Los arts. 15 LPDP y 24 RLPDP establecen que el responsable tendrá la obligación de informar a los titulares de los datos, la información que se recaba de ellos y con qué fines, a través del aviso de privacidad.

Cualquier empresa o ente privado que solicite datos personales deberá elaborar un aviso de privacidad, documento a través del cual se puede conocer la finalidad que tendrá la información que solicitada. El aviso deberá proporcionar además, información que permita identificar a la empresa que recaba los datos y deberá precisar la forma de hacer efectivos los derechos de acceso, rectificación, cancelación y oposición (derechos ARCO). En el aviso de privacidad la empresa deberá consultar a la persona si autoriza que se transfiera su información a terceros. Asimismo, la empresa deberá notificarle de cualquier cambio que realice a dicho aviso de privacidad y pedir su consentimiento para el nuevo uso que quiera dar a los datos. El Aviso de Privacidad podrá ponerse a tu disposición a través de medios físicos, digitales, visuales, sonoros o de cualquier otra tecnología²⁶⁹.

8.3.1 Información que debe de contener el aviso de privacidad

El aviso de privacidad deberá contener al menos la siguiente información (art. 16 LPDP):

1. La identidad y domicilio del responsable que los recaba

²⁶⁸ <http://www.ifai.org.mx/Particulares/faq> (consulta: 09/11/2012).

²⁶⁹ <http://www.ifai.org.mx/Particulares/faq> (consulta: 09/11/2012). A partir de la entrada en vigor de la Ley (al día después de la publicación en el BOE del 05/07/2010), las empresas tuvieron un plazo de un año para expedir el aviso de privacidad.

2. Las finalidades del tratamiento de datos.
3. Las operaciones y medios que el responsable ofrezca a los titulares para limitar el uso o divulgación de los datos.
4. Los medios para ejercer los derechos de acceso, rectificación, cancelación u oposición, de conformidad con lo dispuesto en esta Ley.
5. En su caso, las transferencias de datos que se efectúen.
6. El procedimiento y medio por el cual el responsable comunicará a los titulares de cambios al aviso de privacidad, de conformidad con lo previsto en esta Ley.

En el caso de datos personales sensibles, el aviso de privacidad deberá señalar expresamente que se trata de este tipo de datos.

8.3.2 Formato del aviso de privacidad

El aviso de privacidad debe ponerse a disposición de los titulares a través de formatos impresos, digitales, visuales, sonoros o cualquier otra tecnología, de la siguiente manera (art. 17 LPDP y art. 25 RLPDP):

1. Cuando los datos personales hayan sido obtenidos personalmente del titular, el aviso de privacidad deberá ser facilitado en el momento en que se recaba el dato de forma clara y fehaciente, a través de los formatos por los que se recaban, salvo que se hubiera facilitado el aviso con anterioridad.
2. Cuando los datos personales sean obtenidos directamente del titular por cualquier medio electrónico, óptico, sonoro, visual, o a través de cualquier otra tecnología, el responsable deberá proporcionar al titular de manera inmediata, al menos la información a que se refieren las fracciones I y II del art. 16 LPDP, así como para proveer los mecanismos para que el titular conozca el texto completo del aviso de privacidad (art. 27 RLPDP).

En relación con este dispositivo llama especialmente la opción “cualquier otra tecnología” -del primer párrafo- para el formato del aviso de privacidad. En

ella se aprecia cómo la Ley prevé el avance tecnológico e indirectamente el rezago en el tiempo de la Ley, dejando con ella un amplio margen de interpretación posterior.

Por su parte, el tema del aviso en la Ley federal es innovador, si se considera que otros países, como es el caso español, no cuentan con la previsión expresa del aviso de privacidad en la Ley de la materia, sino en el Reglamento correspondiente.

El aviso de privacidad en México se regula en la Ley y su Reglamento. La Secretaría de Economía, en coadyuvancia con el Instituto, es la responsable de emitir los lineamientos correspondientes para el contenido y alcances del aviso de privacidad. En consecuencia, en junio de 2011 ha sido publicada la Guía práctica para generar el aviso de privacidad (que no los lineamientos), en la que orienta a los responsables del tratamiento de datos personales en la elaboración, diseño y difusión de aviso de privacidad.

La Guía es completa y ejemplifica los requerimientos de la Ley para el aviso. Sin embargo, varía de longitud en completo o simplificado, en función de diversos factores como: el espacio para agregar el aviso (si es limitado o no), el medio por el cual se recaba la información, el tipo de datos que se recogen, si se obtienen de modo directo o indirecto, y si se prevé o no, una transferencia de datos. En este último caso, la autorización esta concebida por *default*, a no ser que, el titular se oponga a la misma marcando la casilla correspondiente.

Por otro lado, cuando el aviso no contempla un espacio suficiente, remite al titular a la búsqueda del aviso completo. Por lo anterior, no es de extrañar que este tema sea poco claro, y que incluso en la remisión que hace al documento completo, conlleve en sí una percepción de poca claridad en la manifestación de la voluntad, convirtiéndose en algo complicado. El aviso de privacidad completo, se parece bastante a un contrato, que ya inspira dificultad en la comprensión, situación que se agrava cuando se está delante de una normativa de nueva implementación, convirtiéndose en un medio poco práctico a efectos de protección del derecho, difusión y concientización.

8.3.3 Datos obtenidos indirectamente del titular y datos con fines históricos, estadísticos o científicos.

Cuando los datos no hayan sido obtenidos directamente del titular, el responsable deberá darle a conocer el cambio en el aviso de privacidad. No resulta esto aplicable, cuando el tratamiento sea con fines históricos, estadísticos o científicos (art. 18 LPDP).

Cuando resulte imposible dar a conocer el aviso de privacidad al titular o exija esfuerzos desproporcionados, en consideración al número de titulares, o a la antigüedad de los datos, previa autorización del Instituto, el responsable podrá instrumentar medidas compensatorias en términos del Reglamento de la LPDP²⁷⁰.

8.4 Calidad

Los datos personales en posesión de empresas deben de estar actualizados y reflejar con veracidad la realidad de la información, de tal manera que cualquier inexactitud no afecte a su titular. Asimismo, implica que el tiempo que la empresa conserve los datos no exceda más allá de lo necesario para el cumplimiento de los fines que justificaron su tratamiento. Cuando se cumpla íntegramente la finalidad para la cual se proporcionaron los datos, el tratamiento deja de ser necesario y, por lo tanto, las empresas deben cancelarlos²⁷¹.

A diferencia de otros ordenamientos, por ejemplo el español, la LPDP mexicana menciona el principio de calidad sin describirlo con posterioridad, sin embargo, se puede ver reflejado a través de la descripción que se hace a los principios de finalidad, lealtad y proporcionalidad.

El Reglamento de esta Ley publicado con posterioridad en diciembre de 2011, establece en el art. 36 RLPDP que se cumple con el principio de calidad cuando los datos personales tratados sean exactos, completos, pertinentes, correctos y actualizados según se requiera para el cumplimiento de la finalidad para la cual son tratados. Señalando que se presume que se cumple con este principio cuando los datos son proporcionados directamente por el titular, y hasta

²⁷⁰ Arts. 33 a 35 RLPDP.

²⁷¹ <http://www.ifai.org.mx/Particulares/faq> (consulta: 09/11/2012).

que éste no manifieste y acredite lo contrario, o bien, el responsable cuente con evidencia objetiva que los contradiga. Cuando los datos personales no fueron obtenidos directamente del titular, el responsable deberá adoptar medidas razonables para que estos respondan al principio de calidad, de acuerdo con el tipo de datos personales y las condiciones del tratamiento. Además, el responsable deberá adoptar los mecanismos que considere necesarios para procurar que los datos personales que trate sean exactos, completos, pertinentes, correctos y actualizados, a fin de que no se altere la veracidad de la información, ni que ello tenga como consecuencia que el titular se vea afectado por dicha situación

8.5 Finalidad

El tratamiento de datos personales deberá limitarse al cumplimiento de las finalidades previstas en el aviso de privacidad. Si el responsable pretende tratar los datos para un fin distinto que no resulte compatible o análogo a los fines establecidos en aviso de privacidad, se requerirá obtener nuevamente el consentimiento del titular (art. 12 LPDP y art. 40 RLPDP).

El responsable deberá distinguir en el aviso de privacidad cuáles son las finalidades que dieron origen y son necesarias para la relación jurídica entre él y el titular, de aquellas que no lo son; para estas últimas, el titular podrá negar o revocar su consentimiento, así como oponerse para el tratamiento de tales finalidades distintas (arts. 41 a 43 RLPDP).

8.6 Lealtad

Este principio se encuentra en el art. 7 LPDP al referir que la obtención de datos personales no debe hacerse a través de medios engañosos o fraudulentos. Y precisar que en todo tratamiento de datos, se presume que existe la expectativa razonable de privacidad, entendida como la confianza que deposita cualquier persona en otra, respecto de que los datos personales proporcionados serán tratados conforme a la LPDP.

El art. 44 RLPDP indica que no se podrán utilizar medios engañosos o fraudulentos para recabar y tratar datos personales. Aclarando que existe una

actuación fraudulenta o engañosa cuando: I. Exista dolo, mala fe o negligencia en la información proporcionada al titular sobre el tratamiento; II. Se vulnere la expectativa razonable de privacidad del titular, o III. Las finalidades no son las informadas en el aviso de privacidad.

8.7 Proporcionalidad

Las empresas o responsables solo podrán recabar los datos estrictamente necesarios para la finalidad que persiguen y que justifica su tratamiento, además deberán realizar esfuerzos razonables para que los datos tratados sean los mínimos necesarios para la realización de dicha finalidad (arts. 45 y 46 RLPDP)²⁷².

El art. 13 LPDP establece que el tratamiento de datos personales será el que resulte necesario, adecuado y relevante en relación con las finalidades previstas en el aviso de privacidad. En particular para datos personales sensibles, el responsable deberá realizar esfuerzos razonables para limitar el período de tratamiento de los mismos a efecto de que sea el mínimo indispensable.

8.8 Responsabilidad

Quienes traten datos personales deben asegurar que ya sea dentro o fuera del país, se cumpla con los principios esenciales de protección de datos personales, comprometiéndose a velar siempre por el cumplimiento de estos principios y a rendir cuentas en caso de incumplimiento²⁷³.

El responsable velará por el cumplimiento de los principios de protección de datos personales establecidos por la Ley, debiendo adoptar las medidas necesarias para su aplicación. Lo anterior aplicará aún y cuando estos datos fueren tratados por un tercero a solicitud del responsable. El responsable deberá tomar las medidas necesarias y suficientes para garantizar que el aviso de privacidad dado a conocer al titular, sea respetado en todo momento por él o por terceros con los que guarde alguna relación jurídica (art. 14 LPDP y art 47 RLPDP).

²⁷² <http://www.ifai.org.mx/Particulares/faq> (consulta: 09/11/2012).

²⁷³ <http://www.ifai.org.mx/Particulares/faq> (consulta: 09/11/2012).

Por su parte, las medidas que el responsable deberá adoptar para garantizar el debido tratamiento, privilegiando los intereses del titular y la expectativa razonable de privacidad son las siguientes (art. 48 RLPDP):

1. Elaborar políticas y programas de privacidad obligatorios y exigibles al interior de la organización del responsable.
2. Poner en práctica un programa de capacitación, actualización y concientización del personal sobre las obligaciones en materia de protección de datos personales.
3. Establecer un sistema de supervisión y vigilancia interna, verificaciones o auditorías externas para comprobar el cumplimiento de las políticas de privacidad.
4. Destinar recursos para la instrumentación de los programas y políticas de privacidad.
5. Instrumentar un procedimiento para que se atienda el riesgo para la protección de datos personales por la implementación de nuevos productos, servicios, tecnologías y modelos de negocios, así como para mitigarlos.
6. Revisar periódicamente las políticas y programas de seguridad para determinar las modificaciones que se requieran.
7. Establecer procedimientos para recibir y responder dudas y quejas de los titulares de los datos personales.
8. Disponer de mecanismos para el cumplimiento de las políticas y programas de privacidad, así como de sanciones por su incumplimiento.
9. Establecer medidas para el aseguramiento de los datos personales, es decir, un conjunto de acciones técnicas y administrativas que permitan garantizar al responsable el cumplimiento de los principios y obligaciones que establece la Ley y el Reglamento.

10. Establecer medidas para la trazabilidad de los datos personales, es decir, acciones, medidas y procedimientos técnicos que permiten rastrear a los datos personales durante su tratamiento.

8.8.1 Seguridad

Un pilar básico y fundamental de un efectivo sistema de protección de datos personales es la garantía de la seguridad de la información, entendida ésta como la implementación de medidas administrativas, físicas y técnicas eficaces para garantizar y velar por la integridad, confidencialidad y disponibilidad de los datos personales. Ello contribuye a minimizar los riesgos de acciones en contra de la información personal como robo, alteración o modificación, pérdida total o parcial, transmisiones indebidas o ilícitas, accesos no autorizados y robo de identidad, entre otras, que pueden lesionar los derechos o libertades fundamentales²⁷⁴.

El art. 19 LPDP establece que 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 (arts. 60 a 66 RLPDP).

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.

8.8.2 Deber de secreto

El art. 21 LPDP señala que el responsable o terceros que intervengan en cualquier fase del tratamiento de datos personales deberán guardar confidencialidad respecto de estos, obligación que subsistirá aun después de finalizar sus relaciones con el titular o, en su caso, con el responsable.

²⁷⁴ <http://www.ifai.org.mx/Particulares/faq> (consulta: 09/11/2012).

8.8.3 Delitos en materia de tratamiento indebido de datos personales

Es relevante, hacer mención del capítulo XI de la LPDP, que refiere los delitos en materia del tratamiento indebido de datos personales, en él se regulan los actos que serán constitutivos de delito en esta área. Esto es una novedad legislativa en materia de protección de datos, ya que no se encuentran tipificados dentro de la Ley de la materia en otros países como España, Argentina, Costa Rica o Perú.

La Ley advierte que los delitos por tratamiento indebido de datos personales será la vulneración de la seguridad a la base de datos. A decir, se prevén dos:

a) Con ánimo de lucro

Cuando el autorizado para tratar datos personales, con ánimo de lucro, provoque una vulneración de seguridad a las bases de datos bajo su custodia. La sanción será de tres meses a tres años y de tratarse de datos personales sensibles, la pena se duplicará.

b) Con ánimo de lucro y a través del engaño

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 transmitirla. La sanción será de seis meses a cinco años y de tratarse de datos personales sensibles, la pena se duplicará.

9. Derechos de los titulares de datos personales

Cualquier titular²⁷⁵, o en su caso su representante legal, podrá ejercer los derechos de: acceso, rectificación, cancelación y oposición (previstos en la LPDP). Por sus iniciales, son conocidos como derechos ARCO. El ejercicio de cualquiera de ellos no es requisito previo ni impide el ejercicio de otro; además estos derechos podrán restringirse por razones de seguridad nacional,

²⁷⁵ Cualquier persona es la titular de sus propios datos personales. El art. 89 del Reglamento establece que para el ejercicio de los derechos ARCO de datos personales de menores de edad o de personas que se encuentren en estado de interdicción o incapacidad establecida por ley, se estará a las reglas de representación dispuestas en el Código Civil Federal.

disposiciones de orden público, seguridad y salud públicas o para proteger los derechos de terceras personas, en los casos y con los alcances previstos en las leyes aplicables en la materia, o bien mediante resolución de la autoridad competente fundada y motivada²⁷⁶.

Los datos personales deben ser resguardados de tal manera que permitan el ejercicio sin dilación de estos derechos (art. 22 LPDP). Por resguardados se puede entender la correcta sistematización de la información para lograr: 1) Tratarlos adecuadamente, 2) Identificarlos con facilidad y 3) Dar trámite a las solicitudes en el plazo previsto. Para ello es importante mantener las medidas de seguridad correspondientes a los datos personales que se poseen.

9.1 Acceso

Los titulares tienen derecho a acceder a los datos personales que de sí mismos obren en poder del responsable²⁷⁷, así como a conocer el aviso de privacidad al que estará sujeto el tratamiento de dicha información (art. 23 LPDP).

La obligación de acceso a la información se dará por cumplida cuando se pongan a disposición del titular los datos personales; o bien, mediante la expedición de copias simples, documentos electrónicos o cualquier otro medio que determine el responsable en el aviso de privacidad²⁷⁸. En el caso de que el titular solicite el acceso a los datos a una persona que presume es el responsable y ésta resulta no serlo, bastará con que así se lo indique a aquél por cualquiera de los medios a que se ha hecho referencia, para tener por cumplida la solicitud (art. 34 LPDP).

²⁷⁶ Art. 87 y 88 RLPDP. Además, véase dentro de este mismo capítulo los límites del derecho.

²⁷⁷ Así como información relativa a las condiciones y generalidades del tratamiento (art. 101 RLPDP).

²⁷⁸ La obligación de acceso se dará por cumplida cuando el responsable ponga a disposición del titular los datos personales en sitio, mediante la expedición de copias simples, medios magnéticos, ópticos, sonoros, visuales u holográficos, o utilizando otras tecnologías de la información que se hayan previsto en el aviso de privacidad. En todos los casos, el acceso deberá ser en formatos legibles o comprensibles para el titular (art. 102 RLPDP).

9.2 Rectificación

Es el derecho que otorga la Ley para que el titular solicite al responsable en cualquier momento se corrijan los datos personales, y se ejercita cuando la información sea incorrecta, imprecisa, inexacta, incompleta o esté desactualizada (arts. 24 LPDP y 103 RLPDP).

Cuando el titular solicite la rectificación de datos personales deberá indicar las modificaciones a realizar y aportar la documentación que sustente su petición²⁷⁹ (arts. 31 LPDP y 104 RLPDP).

9.3 Cancelación

Es la facultad que otorga la Ley para solicitar la cancelación de los datos personales contenidos en las bases que tenga una determinada empresa, la cual deberá dejar de tratar dicha información, en especial cuando el tratamiento no cumpla con las disposiciones legales aplicables. Los datos deberán ser bloqueados y, posteriormente, suprimidos de las bases de datos.

El art. 25 LPDP establece lo anterior y dice que el titular de los datos tendrá en todo momento el derecho a cancelar sus datos personales. La cancelación de estos, dará lugar a un periodo de bloqueo tras el cual se procederá a la supresión del dato. El responsable podrá conservarlos exclusivamente para efectos de las responsabilidades nacidas del tratamiento. El periodo de bloqueo será equivalente al plazo de prescripción de las acciones derivadas de la relación jurídica que funda el tratamiento en los términos de la Ley aplicable en la materia; y su propósito es impedir el tratamiento, a excepción del almacenamiento, o posible acceso por persona alguna, salvo que alguna disposición legal prevea lo contrario²⁸⁰.

Una vez cancelado el dato se dará aviso a su titular. Cuando los datos personales hubiesen sido transmitidos con anterioridad a la fecha de rectificación o cancelación y sigan siendo tratados por terceros, el responsable deberá

²⁷⁹ Además de indicar lo estipulado por el art. 29 LPDP.

²⁸⁰ Arts. 107 y 108 RLPDP respecto del procedimiento del bloqueo.

informarles de dicha solicitud de rectificación o cancelación, para que procedan a efectuarla también.

En cuanto a las excepciones al derecho de cancelación, el art. 26 LPDP precisa que el responsable no estará obligado a cancelar los datos personales cuando:

1. Se refiera a las partes de un contrato privado, social o administrativo y sean necesarios para su desarrollo y cumplimiento.
2. Deban ser tratados por disposición legal.
3. Obstaculice actuaciones judiciales o administrativas vinculadas a obligaciones fiscales, la investigación y persecución de delitos o la actualización de sanciones administrativas.
4. Sean necesarios para proteger los intereses jurídicamente tutelados del titular.
5. Sean necesarios para realizar una acción en función del interés público.
6. Sean necesarios para cumplir con una obligación legalmente adquirida por el titular.
7. Sean objeto de tratamiento para la prevención o para el diagnóstico médico o la gestión de servicios de salud, siempre que dicho tratamiento se realice por un profesional de la salud sujeto a un deber de secreto.

9.4 Oposición

El titular tendrá derecho en todo momento y por causa legítima a oponerse al tratamiento de sus datos. De resultar procedente, el responsable no podrá tratar los datos relativos al titular (art. 27 LPDP)²⁸¹, cuando:

²⁸¹ No procederá el ejercicio del derecho de oposición en aquellos casos en los que el tratamiento sea necesario para el cumplimiento de una obligación legal impuesta al responsable (art. 109 RLPDP).

- Exista causa legítima y su situación específica así lo requiera, lo cual debe justificar que aun siendo lícito el tratamiento, el mismo debe cesar para evitar que su persistencia cause un perjuicio al titular.
- Requiera manifestar su oposición para el tratamiento de sus datos personales a fin de que no se lleve a cabo el tratamiento para fines específicos.

En cuanto al ejercicio del derecho de oposición, el art. 110 del RLPDP contempla que los responsables, podrán gestionar listados de exclusión propios en los que incluyan los datos de las personas que han manifestado su negativa para que trate sus datos personales, ya sea para sus productos o de terceras personas. Asimismo, los responsables podrán gestionar listados comunes de exclusión por sectores o generales²⁸².

Actualmente, en México existen registros de exclusión, producto principalmente de las incomodas y múltiples llamadas que durante varios años, las personas recibían diariamente a sus hogares para el ofrecimiento de productos ofertados por entidades bancarias. Así, El Registro Público de Consumidores previsto en la Ley Federal de Protección al Consumidor y el Registro Público de Usuarios previsto en la Ley de Protección y Defensa al Usuario de Servicios Financieros, continuarán vigentes y se registrarán de conformidad con lo que establezcan las leyes en cita y las disposiciones aplicables que ellas deriven.

9.5 Procedimiento de solicitud de los derechos ARCO

Para ejercitar los derechos de acceso, rectificación, cancelación y oposición es necesario seguir un procedimiento de solicitud ante quien posea la información, este es un trámite que puede llevarse a cabo por cualquier persona y sin necesidad de tener conocimientos especializados en la materia. Es destacable esta cualidad porque estamos ante el ejercicio de un derecho fundamental y como tal debe de estar al alcance de cualquier individuo.

²⁸² En ambos casos, la inscripción del titular a dichos listados deberá ser gratuita y otorgar al titular una constancia de su inscripción la mismo, a través de mecanismos que el responsable determine.

9.5.1 Solicitud

El ejercicio de los derechos ARCO se hará mediante la *solicitud* a la empresa o responsable del tratamiento de datos personales, que deberá contener y acompañar lo siguiente (art. 29 LPDP)²⁸³:

1. El nombre del titular y domicilio u otro medio para comunicarle la respuesta a su solicitud.
2. Los documentos que acrediten la identidad o, en su caso, la representación legal del titular.
3. La descripción clara y precisa de los datos personales respecto de los que se busca ejercer alguno de los derechos ARCO.
4. Cualquier otro elemento o documento que facilite la localización de los datos personales²⁸⁴.

Por otros elementos o documentos que faciliten la localización se pueden señalar como ejemplos: la finalidad del tratamiento, fecha de recolección de la información, razón por la cual se desea ejercitar el derecho, documentación recibida por el responsable al momento de recabar los datos o durante el tratamiento, etc.

²⁸³ Es importante conservar la constancia de la solicitud que se presenta, pues si no se obtiene respuesta o la persona no queda satisfecha, podrá acudir al Instituto Federal de Acceso a la Información Pública y Protección de Datos (IFAI), y para ello la constancia será indispensable. El art. 88 RLPDP, establece que los derechos ARCO se ejercerán: I. Por el titular, previa acreditación de su identidad, a través de la presentación de copia de su documento de identificación y habiendo exhibido el original para su cotejo. También podrán ser admisibles los instrumentos electrónicos por medio de los cuales sea posible identificar fehacientemente al titular, u otros mecanismos de autenticación permitidos por otras disposiciones legales o reglamentarias, o aquellos previamente establecidos por el responsable. La utilización de firma electrónica avanzada o del instrumento electrónico que los sustituya eximirá de la presentación de la copia del documento de identificación, y II. Por representante del titular, previa acreditación de: a) La identidad del titular; b) La identidad del responsable, y c) la existencia de la representación, mediante instrumento público o carta poder firmada ante dos testigos, o declaración en comparecencia personal del titular. Para el ejercicio de los derechos ARCO de datos personales de menores de edad o de personas que se encuentren en estado de interdicción o incapacidad establecida por ley, se estará a las reglas de representación dispuestas en el Código Civil Federal.

²⁸⁴ En caso de la que información sea errónea o insuficiente, se requerirá al titular para que proporcione adicionalmente lo que proceda, para lo cual contará con 10 días para hacerlo (art. 96 RLPDP).

Para un correcto proceso de respuesta y trámite a estas solicitudes, todo responsable deberá designar una persona o departamento de datos personales, para el ejercicio de los derechos ARCO²⁸⁵. Asimismo fomentará la protección de datos personales al interior de la organización (art. 30 LPDP).

9.5.2 Negativa de solicitud

El responsable podrá *negar la solicitud* de los derechos ARCO, en los siguientes supuestos (art. 34 LPDP):

1. Cuando el solicitante no sea el titular de los datos personales o el responsable legal no esté debidamente acreditado para ello.
2. Cuando en su base de datos no se encuentren los datos personales del solicitante.
3. Cuando se lesionen los derechos de un tercero.
4. Cuando exista un impedimento legal o la resolución de una autoridad competente que restrinja el ejercicio de los derechos ARCO.

Asimismo, la ley establece la existencia de dos tipos de negativa que son la parcial y la absoluta, cuyos efectos son:

1. Parcial: su efecto es que el responsable efectúe la solicitud.
2. Absoluta²⁸⁶: produce que el responsable tenga el deber de informar el motivo de su decisión y la comunique al titular de los datos, o en su caso, al representante legal, en los plazos establecidos para tal efecto²⁸⁷, por el mismo medio por el que se llevó a cabo la solicitud, acompañando, en su caso, las pruebas que resulten pertinentes.

²⁸⁵ El art. 32 LPDP establece que el responsable comunicará al titular de los datos en el plazo máximo de 20 días contados desde la fecha en que se recibió la solicitud de algún derecho ARCO. La determinación adoptada, en el caso de ser procedente, se hará efectiva dentro de los 15 días siguientes a la fecha en que se comunique. En el caso de las solicitudes de acceso, procederá la entrega previa acreditación de la identidad del solicitante o representante legal. Estos plazos, en caso de justificación, podrán ser ampliados una sola vez por un periodo igual.

²⁸⁶ El art. 34 LPDP no la define como absoluta, sin embargo, al precisar la “parcial” es sencillo deducir que la otra será la que referimos como “absoluta”.

²⁸⁷ Los plazos son los establecidos por el art. 32 LPDP.

9.5.3 Costo legal

La Ley indica que la entrega de los datos personales será gratuita, debiendo cubrir el titular únicamente los gastos justificados de envío o con el costo de reproducción en copias u otros formatos.

Dicho derecho –de acceso- se ejercerá por el titular en forma gratuita, previa acreditación de su identidad ante el responsable. No obstante, si la misma persona reitera su solicitud en un periodo menor de doce meses, los costos no serán mayores a tres días de salario mínimo general vigente en el Distrito Federal, a menos que existan modificaciones sustanciales al aviso de privacidad que motiven nuevas consultas (art. 35 LPDP)²⁸⁸.

En este sentido, se observa que la Ley establece que el ejercicio del derecho de acceso será gratuito. Lo anterior, se entiende como una especie de “principio de gratuidad” que se puede invocar cuando se ejercita un derecho ARCO, con la salvedad de que será así, siempre y cuando, dicho ejercicio sea por una sólo vez dentro de los doce meses, es decir, una vez por año. La gratuidad se encuentra prevista para incentivar al ciudadano a ejercer este derecho, mientras que el término de un año es comprensible, en el sentido de que la persona no haga un uso indiscriminado del ejercicio del derecho de acceso.

10. Normatividad aplicable

Hasta hace un par de años, la regulación en la materia era insuficiente, por no decir nula, al no encontrarse regulada en el ámbito federal, mediante una Ley. Esto se debía a que las iniciativas propuestas por los diferentes partidos políticos no habían prosperado. La labor del Instituto, aunque limitada, se puede considerar loable hasta entonces, ya que en la medida de sus posibilidades emitió lo que estuvo a su alcance, mediante diversos instrumentos como los *lineamientos* y *recomendaciones*.

²⁸⁸ El art. 93 RLPDP establece que el ejercicio de los derechos ARCO será sencillo y gratuito, debiendo cubrir el titular únicamente los gastos de envío, reproducción y, en su caso, certificación de documentos, salvo la excepción prevista en el segundo párrafo del art. 35 LPDP (si lo pide más de una vez en doce meses). Los costos de reproducción no podrán ser mayores a los costos de recuperación del material correspondiente. El responsable no podrá establecer como única vía para la presentación de las solicitudes del ejercicio de los derechos ARCO algún servicio o medio con costo.

Desde que se emitió la LAI en 2002²⁸⁹, el derecho a la protección de datos personales se encontraba tímidamente previsto porque se encontraba regulado en escuetos siete artículos del Capítulo IV de dicha Ley, que aplica solo al sector público. Posteriormente en 2007 y 2009 con las reformas hechas a la Constitución mexicana. Estos cambios en la Carta Magna abrirían paso para que el Congreso Federal emitiera la actual Ley Federal de Protección de Datos Personales en Posesión de Particulares, publicada en el DOF en 2010.

Es así que la normatividad de la materia se encuentra contenida en los siguientes documentos:

- Constitución Política de los Estados Unidos Mexicanos.
- Ley Federal de Protección de Datos Personales en posesión de Particulares.
- Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental
- Reglamento de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental.
- Lineamientos de Protección de Datos Personales.
- Lineamientos que deberán observar las dependencias y entidades de la Administración Pública Federal en la recepción, procesamiento, trámite, resolución y notificación de las solicitudes de corrección de datos personales que formulen los particulares.
- Lineamientos que deberán observar las dependencias y entidades de la Administración Pública Federal en la recepción, procesamiento y trámite de las solicitudes de acceso a la información gubernamental que formulen los particulares, así como en su resolución y notificación, y la entrega de la información en su caso, con exclusión de las solicitudes de acceso a datos y su corrección.

²⁸⁹ La Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental se publicó en el DOF el día 11 de junio de 2002 y entró en vigor al día siguiente.

- Lineamientos que deberán observar las dependencias y entidades de la Administración Pública Federal en la recepción, procesamiento, trámite, resolución y notificación de las solicitudes de acceso a datos personales que formulen los particulares con exclusión de las solicitudes de corrección de dichos datos.
- Lineamientos que deberán observar las dependencias y entidades de la Administración Pública Federal para notificar al Instituto el listado de sus sistemas de datos personales.
- Recomendaciones sobre medidas de seguridad aplicables a los sistemas de datos personales.

10.1 Constitución Política de los Estados Unidos Mexicanos.

En relación al derecho de protección de datos personales, en México sólo se contaba con el Capítulo IV de la LAI de 2002; y no es sino hasta el 20 de julio de 2007 que se publica en el DOF la reforma del art. 6 CPM (de 13 de junio de 2007), en la que se reconoce a nivel constitucional, no sólo el derecho de acceso a la información, sino también, el derecho fundamental a la protección de los datos personales. Es así que, esta prerrogativa, tomaba su inaplazable importancia dentro de la Carta Magna²⁹⁰.

Es importante señalar que las fracciones de este artículo son *principios y bases* que rigen al sector público cuando el ciudadano haya de ejercer su derecho de acceso a la información. El texto menciona que se habrán de proteger la vida privada y los datos personales, en los términos que fijen las leyes. Actualmente, la LAI contiene las disposiciones correspondientes en la materia y es de aplicación a la Federación, los Estados y el Distrito Federal, ya que la LPDP atañe de manera exclusiva los datos en posesión de particulares.

²⁹⁰ “Artículo 6. ... Para el ejercicio del derecho de acceso a la información, la Federación, los Estados y el Distrito Federal, en el ámbito de sus respectivas competencias, se regirán por los siguientes principios y bases: I...; II. La información que se refiere a la vida privada y los datos personales será protegida en los términos y con las excepciones que fijen las leyes; III. Toda persona, sin necesidad de acreditar interés alguno o justificar su utilización, tendrá acceso gratuito a la información pública, a sus datos personales o a la rectificación de estos; IV...”

Esta reforma, solo reconoce dos derechos ARCO, el de acceso y rectificación, mientras que el de cancelación y oposición fueron omitidos y es de considerar una omisión que puede dar lugar a que el administrador, en sus tareas diarias –que no son pocas-, se respalde para no cancelar o aceptar la oposición cuando proceda²⁹¹. Este dispositivo, no ordena a la Federación, los Estados y el DF de la debida observancia de la gama de derechos comprendidos en el derecho a la protección de datos personales. Actualmente, si bien los derechos ARCO están desarrollados en la LPDP, también hay que precisar, que ésta no rige para el sector público, por lo que no es invocable ante una posible vulneración de ellos por parte de un ente público.

A partir del año 2009 los derechos de acceso, rectificación, cancelación y oposición, son garantías del ciudadano por orden del actual art. 16 CPM. Es de considerar necesaria una reforma de la LAI para introducir los derechos ARCO, aunque lo más conveniente sería la emisión de una Ley Federal de Protección de Datos Personales en posesión del sector público, que regule también el derecho de cancelación y oposición para no crear lagunas legales. En relación con la reforma a este dispositivo, es de señalar como dota al sector público de una ventaja, de un poder para poseer las bases de datos actualizadas (mediante el derecho de corrección) y no permitir al ciudadano la petición de cancelación²⁹². De la redacción del artículo no se desprende la posibilidad de que el sector público se deshaga de la información, previa petición, cuando los datos no sean necesarios²⁹³.

Se reconoce el esfuerzo del legislador por haber dado un paso muy significativo en la materia, ya que es la primera vez que se reconoce

²⁹¹ El ejercicio de estos derechos si procedería porque el artículo 16 los señala como garantías de este derecho, sin distinguir si serán oponibles en contra del sector privado o el público.

²⁹² Lo que es normal en casos que conciernen a la Procuraduría General de la República, la Hacienda Pública, etc., pero esto no se justificaría, por ejemplo, en el caso de apertura de expedientes por error.

²⁹³ “Artículo 16. Nadie puede ser molestado en su persona, familia, domicilio, papeles o posesiones, sino en virtud de mandamiento escrito de la autoridad competente, que funde y motive la causa legal del procedimiento. 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. (...)”

constitucionalmente el derecho a la protección de datos personales, que es una garantía real de todo individuo a la protección de su información frente a intromisiones de terceros. Es de señalar que el derecho fue correctamente ubicado en el Título I, Capítulo I de la CPM, referente a las Garantías Individuales²⁹⁴, que es el apartado dedicado a la protección de lo que en otros instrumentos se denomina como “derechos fundamentales”.

Es importante aclarar que hasta antes de la reforma del art. 16 CPM²⁹⁵, el derecho a la protección de datos personales, concernía únicamente a aquellos que estuviesen en manos del sector público federal, ya que el art. 6 CPM inicia así²⁹⁶: “para el ejercicio del derecho de acceso a la información, la Federación, los Estados y el Distrito Federal, en el ámbito de sus respectivas competencias, se regirán por los siguientes principios y bases: I)...”. De esta manera, esta reforma adolecía del reconocimiento del derecho frente a las vulneraciones que proviniesen del sector privado, que es básicamente el que infringe a diario la vida privada de las personas. Esto último, también Gómez-Robledo Verduzco y Ornelas Núñez (2006: 27) lo refieren en su obra *Protección de Datos Personales en México*, cuando hacen abordan la Ley General de Salud, y acentúan que más de la mitad de la población en México es atendida por instituciones particulares que no están vinculadas a la LAI y por tanto no son sujetos obligados de su capítulo referente a la protección de datos personales.

En cuanto a la materia que hoy nos ocupa, la Constitución mexicana hubo de ser reformada en su art. 73, adicionando la fracción XXIX-O²⁹⁷, la cual dota de facultades al Congreso para legislar en materia de protección de datos personales en posesión de los particulares²⁹⁸.

²⁹⁴ En el apartado sobre Garantías Individuales se contienen descritos los derechos fundamentales en la Constitución mexicana.

²⁹⁵ La reforma es de 21 de abril de 2009 y fue publicada en el DOF el 1º de junio del mismo año, mediante la cual se reforma el segundo párrafo.

²⁹⁶ Esta reforma es del día 13 de junio de 2007 y fue publicada en el DOF el 20 de julio del mismo año.

²⁹⁷ La reforma es de 24 de marzo de 2009 y fue publicada en el DOF el 30 de abril del mismo año.

²⁹⁸ “Artículo 73. El Congreso tiene facultad: (...); XXIX-O. Para legislar en materia de protección de datos personales en posesión de particulares; (...)”

En este sentido se ha visto cómo la CPM hubo de beneficiarse de tres reformas significativas para la protección de este derecho fundamental, sin las cuales hoy en día no sería posible ejercitar este derecho de tercera generación.

10.2 Ley Federal de Protección de Datos Personales en Posesión de los Particulares

Desde el año 2001 fueron presentadas en el Congreso Federal un total de nueve iniciativas, ninguna de ellas prosperó, ni concilio los intereses y necesidades de los distintos sectores involucrados. Es hasta el año 2002 en que se publica la Ley Federal de Transparencia y Acceso a información Pública Gubernamental, reconociéndose por primera vez el derecho a la protección de datos personales, que constriñe a todos los entes públicos federales a cumplir con una serie de reglas básicas encaminadas a garantizar el debido tratamiento de la información personal que poseen para llevar a cabo sus actividades cotidianas.

Luego, en el año 2007 se reforma el art. 6 de la Constitución Política de los Estados Unidos Mexicanos, mediante la cual aparece escrito por primera vez en la Carta Magna el derecho a la protección de datos personales. Finalmente en el año 2009 se llevan a cabo las últimas reformas constitucionales en la materia, que corresponden a los arts. 16 y 73 CPM para regular aquella información en posesión de los particulares²⁹⁹.

La aprobación de la Ley Federal de Protección de Datos Personales en posesión de los Particulares por el Congreso Federal se da tras años de debates sobre la conveniencia y contenido de una ley en esta materia. Luego de sentadas las bases constitucionales, la Comisión de Gobernación de la Cámara de Diputados de la LXI Legislatura, se da a la tarea de elaborar un proyecto de ley que satisfaga las necesidades y demandas fundamentales de todos los actores involucrados, a fin de contar con una ley consensuada en todos los sentidos. Una vez culminada esta tarea, el 13 de abril de 2010 el Pleno de la Cámara de Diputados aprobó el dictamen presentado por la Comisión de Gobernación,

²⁹⁹ El art. 16 CPM incorpora a la lista de garantías fundamentales consagradas en nuestra Carta Magna, el derecho a la protección de datos personales y lo dota de contenido. Por su parte el art. 73 CPM otorga facultades al Congreso de la Unión para legislar en materia de protección de datos personales en posesión de particulares.

turnando la minuta de ley aprobada a la Cámara de Senadores para su valoración. Es así que las Comisiones de Gobernación y de Estudios Legislativos de la Cámara de Senadores, hacen el estudio y valoración de dicha minuta y someten a votación del Pleno el dictamen correspondiente, aprobándolo por unanimidad de los senadores presentes el 27 de abril de 2010³⁰⁰.

La LPDP es el resultado de la necesidad en México de una ley que regulara la materia y cumpliera con los estándares actuales a nivel internacional en materia de protección de datos personales. En el caso de la Unión Europea la directiva 95/46/CE establece que en el ámbito de las relaciones comerciales, únicamente se podrá realizar intercambio de datos personales con los países que mantengan un nivel adecuado de protección en la materia, de lo contrario habría que pedirse un permiso especial al organismo regulador (por ejemplo en España habría de pedirse el permiso a la Agencia Española de Protección de Datos). Lo anterior, hace notar que el que México no contara con una Ley de Protección de Datos, entorpecía las relaciones comerciales.

Es de destacar que las primeras leyes de protección de datos surgen en el mundo en la década de los 70's. Entre estas leyes se encuentra la ley sueca de 11 de mayo de 1973, la alemana de 27 de enero de 1977, la ley francesa del 6 de enero de 1978, las leyes danesas del 8 de junio de 1978, la ley noruega del 9 de junio de 1978, la ley austriaca del 18 de octubre de 1978 y la ley de Luxemburgo de 31 de marzo de 1979.

También se necesitaba de una ley federal que homogenizara las distintas regulaciones estatales que existían en la materia. El país contaba, hasta antes de la publicación de la LPDP, con la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental, que hacía una leve mención en solo siete artículos del derecho a la protección de datos personales en posesión del sector público.

³⁰⁰ <http://www.privacyconference2011.org/#> (consulta: 09/11/2012).

México cuenta con 31 estados y un Distrito Federal, de estos solo siete contaban con una regulación estatal de la protección de datos (Coahuila, Colima, Distrito Federal, Guanajuato, Morelos, Oaxaca y Tlaxcala)³⁰¹.

10.3 Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares

Este instrumento (RLPDP) se firmó el 19 de diciembre de 2011 y publicado en el DOF el 21 de diciembre de 2011. Se compone de 144 artículos los cuales están organizados en diez capítulos, que son:

- I. Disposiciones generales: objeto, definiciones, ámbito de aplicación, ámbito territorial de aplicación, información de personas físicas con actividad comercial y datos de representación y contacto, tratamiento derivado de una relación jurídica, grupos sin personalidad jurídica.
- II. De los principios de protección de datos personales: principio de ilicitud, principio de consentimiento, características del consentimiento, consentimiento tácito, solicitud del consentimiento tácito, consentimiento expreso, solicitud del consentimiento del consentimiento expreso, excepciones al principio del consentimiento, consentimiento verbal, consentimiento escrito, prueba para demostrar la obtención del consentimiento, revocación del consentimiento, procedimiento ante la negativa al cese en el tratamiento, principio de información, características del aviso de privacidad, medios de difusión, elementos del aviso de privacidad, aviso de privacidad para la obtención directa de los datos personales, aviso de privacidad en formatos con espacio limitado, aviso de privacidad para obtención indirecta de datos personales, tratamiento para fines mercadotécnicos, publicitarios o de prospección comercial, prueba del aviso de privacidad, medidas compensatorias, solicitud para autorización de

³⁰¹ Ley de Acceso a la Información Pública y Protección de Datos Personales para el Estados de Coahuila, Ley de Protección de Datos del Estado de Colima, Ley de Protección de Datos Personales para el Distrito Federal, Ley de Protección de Datos Personales para el Estado y los municipios de Guanajuato, Ley de Información Pública Estadística y Protección de Datos Personales del Estado de Morelos, Ley de Protección de Datos Personales (Oaxaca), Ley de Acceso a la Información Pública y Protección de Datos Personales para el Estado de Tlaxcala.

medidas compensatorias, procedimiento para la autorización de medidas compensatorias, modalidades de medidas compensatorias, principio de calidad, plazos de conservación de los datos personales, procedimiento para conservación, bloqueo y supresión de los datos personales, prueba del cumplimiento de los plazos de conservación, principio de finalidad, diferenciación de finalidades, oposición del tratamiento para finalidades distintas, principio de lealtad, principio de proporcionalidad, criterio de minimización, principio de responsabilidad, medidas para el principio de responsabilidad, figura del encargado, obligaciones del encargado, relación entre el responsable y el encargado, tratamiento de datos personales en el denominado cómputo en la nube, remisiones de datos personales, subcontratación de servicios, autorización de subcontratación y, supuestos para la creación de bases de datos personales sensibles.

- III. De las medidas de seguridad en el tratamiento de datos personales: alcance, atenuación de sanciones, funciones de seguridad, factores para determinar las medidas de seguridad, acciones para la seguridad de los datos personales, actualización de las medidas de seguridad, vulneraciones de seguridad, notificación de vulneraciones de seguridad, información mínima al titular en caso de vulneraciones de seguridad.
- IV. De las transferencias de datos personales: alcance, condiciones para la transferencia, prueba del cumplimiento de las obligaciones en materia de transferencias, transferencias dentro del mismo grupo del responsable, condiciones específicas para las transferencias nacionales, receptor de los datos personales, formalización de las transferencias nacionales, condiciones específicas para las transferencias internacionales, formalización de las transferencias internacionales, opinión del instituto respecto de las transferencias.
- V. De la coordinación entre autoridades: emisión de regulación secundaria y mecanismos de coordinación.

- VI. De la autorregulación vinculante: objeto de la autorregulación, objetivos específicos de la autorregulación, incentivos para la autorregulación, contenido mínimo de los esquemas de autorregulación, certificación en protección de datos personales, personas físicas o morales acreditadas, parámetros de autorregulación, registro de esquemas de autorregulación.
- VII. De los derechos de los titulares de datos personales y su ejercicio: ejercicio de los derechos, restricciones al ejercicio de los derechos, personas facultadas para el ejercicio de los derechos, medios para el ejercicio de los derechos, servicios de atención al público, procedimientos específicos para el ejercicio de los derechos ARCO, costos, domicilio del titular, registro de solicitudes, requerimiento de información adicional, ampliación de plazos, respuesta por parte del responsable, derecho de acceso, medios para el cumplimiento del derecho de acceso, derecho de rectificación, requisitos para el ejercicio del derecho de rectificación, derecho de cancelación, ejercicio del derecho de cancelación, bloqueo, propósitos de bloqueo, derecho de oposición, listados de exclusión, registro público de consumidores y registro público de usuarios, tratamiento de datos personales en decisiones sin intervención humana valorativa.
- VIII. Del procedimiento de protección de derechos: inicio, medios para presentar la solicitud de protección de derechos, causales de procedencia, requisitos de la solicitud de protección de derechos, acuerdo de admisión, admisión o desechamiento de las pruebas, ofrecimiento de pruebas, conciliación, audiencia, presentación de alegatos, tercero interesado, falta de respuesta, resoluciones, medios de impugnación, reconducción del procedimiento.
- IX. Del procedimiento de verificación: inicio, causales de procedencia, fe pública, requisitos de la denuncia, desarrollo de verificación, visitas de verificación, identificación del personal verificador, acta de

verificación, contenido de las actas de verificación, resolución, medios de impugnación, reconducción del procedimiento.

- X. Del procedimiento de imposición de sanciones: inicio, ofrecimiento y desahogo de pruebas, admisión o desechamiento de las pruebas, cierre de instrucción y resolución, medios de impugnación.

10.4 Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental

Actualmente y como se ha dicho con anterioridad la protección de datos personales, se encontraba contenida en un capítulo de apenas siete artículos dentro de la LAI (arts. 20 a 26), regulación que no era suficientemente clara y que mucho menos brindaba de una completa seguridad jurídica a las personas que se vieran violentadas por la vulneración a su privacidad a través de sus datos personales.

Entre los objetivos de ésta ley se encuentra el de garantizar la protección de los datos personales en posesión de los sujetos obligados. Así mismo, ésta se limita a señalar de manera muy general las responsabilidades de los sujetos obligados, los casos en que no se requerirá el consentimiento de los individuos para proporcionar los datos personales, que los sujetos obligados que posean un sistema de base de datos deberán de comunicarlo al Instituto, que los individuos podrán solicitar gratuitamente los datos que de ellos obren en los ficheros, y que así también podrán pedir motivadamente la modificación de sus datos³⁰².

10.5 Reglamento de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental

Este documento es publicado en el DOF el 21 de diciembre de 2011, y a diferencia de la LAI, el reglamento es más explícito en lo que hace a la regulación y procedimientos que deberán seguirse en lo que se refiere a datos personales.

³⁰² Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental (Artículos 20 a 26).

El referido reglamento en su capítulo VIII, referente a la protección de datos personales, en su artículo 47, hace mención de que los procedimientos para acceder a los datos en posesión de las dependencias deberán garantizar la protección de los derechos de los individuos a la vida privada y a la intimidad, así como el acceso y corrección de su datos personales. Así también este capítulo en su artículo 48, nos refiere de la publicidad que el Instituto habrá de hacer de las bases de datos, que previamente le comuniquen las dependencias y entidades.

Por otro lado, en el capítulo XIII, relativo a los procedimientos de acceso y corrección de datos personales, del artículo 76 al 81 se desprenden detalladamente las formas que habrán de seguirse para acceder a los datos personales que de un individuo se contengan en una base de datos; así como el procedimiento que habrá de seguirse cuando los datos que se contengan en ésta sean incorrectos.

10.6 Lineamientos de Protección de Datos Personales

Estos lineamientos tienen por objeto establecer las políticas generales y procedimientos que deberán observar las dependencias y entidades de la Administración Pública Federal para garantizar a la persona la facultad de decisión sobre el uso y destino de sus datos personales, con el propósito de asegurar su adecuado tratamiento e impedir su transmisión ilícita y lesiva para la dignidad y derechos del afectado. Para tal efecto, este ordenamiento establece las condiciones y requisitos mínimos para el debido manejo y custodia de los sistemas de datos que se encuentren en posesión de la administración Pública Federal en el ejercicio de sus atribuciones.

11. Criterio de la Suprema Corte de Justicia de la Nación sobre la vida privada.

Con relación al derecho a la *intimidad* en México, la Suprema Corte de Justicia de la Nación, establece que “*el derecho a la intimidad es la facultad que le reconoce el Estado al hombre, de mantener reservada la información que*

considerare no comunicable”³⁰³. En esta misma ejecutoria, la Corte asienta que los artículos 14 y 16 constitucionales garantizan con amplitud la vida privada del individuo, su familia, su domicilio y sus posesiones, como un límite no sólo frente a otro derecho sino también frente a la autoridad, por constituir tales aspectos, valores esenciales de respeto entre gobierno-gobernado, de tal forma que la libertad de las personas, para decidir lo relativo a su cuerpo y a su integridad personal se encuentra, en todo momento, guarecida por el Estado, aun cuando existen casos en que el Estado puede justificar la limitación de estos derechos.

En lo que hace a la vida privada, existe otro análisis que la Corte hace al respecto (partiendo de su reflexión sobre el honor), en donde confusamente la señala como una parte de la intimidad, y termina mencionando ambos conceptos como sinónimos mediante la conjunción “o”³⁰⁴. La redacción literal es: *“Entre tales beneficios también se encuentra la vida privada de la intimidad personal. Ésta es un conjunto de bienes que pertenecen a la esfera secreta de cada persona, pues no conciernen al conocimiento público, y este deber de respeto a la intimidad o vida privada está íntimamente relacionado con el derecho al honor”*.

Asimismo, es interesante el caso de las personas morales, a quienes se les atribuye una especie de honor, mediante la denominación de “reputación”. Lo anterior, se desprende de la Jurisprudencia al establecer la reparación del daño moral, para las personas colectivas, reconociéndoles de igual forma que a las personas físicas, la afectación que pueden sufrir en su reputación y a la consideración que de sí misma tienen los demás. La Sentencia precisa que es

³⁰³ Ejecutoria con número de registro 20018, consultada en el Semanario Judicial de la Federación. Novena Época. Tomo XXV, Marzo 2007, p. 112. Es Jurisprudencia por contradicción de tesis número 1a./J. 99/2006, aprobada por la Primera Sala en fecha 22 de noviembre de 2006, consultada en el Semanario Judicial referido con anterioridad, p. 150.

³⁰⁴ Ejecutoria con número de registro 18765, de la Jurisprudencia por contradicción de tesis número 1a./J. 6/2005, aprobada por la Primera Sala en fecha 26 de enero de 2005. Así mismo, se refiere al honor apuntando que entre los bienes fundamentales que pueden lesionarse con el daño moral se ubica el honor, que consiste en la reputación, en el buen nombre y en la estimación social que una persona ha podido ganarse para sí, y desde el punto de vista subjetivo es el sentimiento de la estimación que cada persona tiene para sí misma. Además, precisa que el honor es también la dignidad personal que se manifiesta en la consideración de los terceros y en el sentimiento de respeto y dignidad que cada persona tiene de ella.

jurídicamente posible que las personas colectivas demanden la reparación del daño moral que llegare a ocasionárseles, y obliga al responsable a repararlo mediante una indemnización pecuniaria. Además, señala que si el derecho les atribuye la calidad de personas morales a esas colectividades que adquieren unidad y cohesión a través de la personalidad, permitiéndoles así adquirir individualidad de manera similar al ser humano, es indudable que por analogía, los conceptos relativos a la reputación y a la consideración que de sí misma tienen los demás, también se aplican a las personas morales³⁰⁵.

12. Criterio de la Suprema Corte de Justicia de la Nación sobre el derecho a la protección de datos personales.

La SCJN en México a la fecha ha emitido distintos criterios en tesis. En un criterio de 2009, la Corte señala que el hacer uso de la fotografía de una persona que no ha sido puesta a disposición del Ministerio Público en calidad de detenida o presunto responsable, constituye un acto de molestia al hacer uso de su imagen. Ante esto, el Estado podría estar violando derechos humanos si incumple con las obligaciones relativas a la protección de datos personales, que consisten en: a) solicitar o registrar información que contenga datos personales sólo en los casos previstos por la ley; y, b) tratar confidencialmente tales datos, lo que implica

³⁰⁵ *DAÑO MORAL. LAS PERSONAS MORALES ESTÁN LEGITIMADAS PARA DEMANDAR SU REPARACIÓN EN CASO QUE SE AFECTE LA CONSIDERACIÓN QUE TIENEN LOS DEMÁS RESPECTO DE ELLAS (ARTÍCULO 1916 DEL CÓDIGO CIVIL PARA EL DISTRITO FEDERAL). Conforme al citado precepto, es jurídicamente posible que las personas colectivas demanden la reparación del daño moral que llegare a ocasionárseles, ya que al definirlo como la afectación que una persona sufre en sus sentimientos, afectos, creencias, decoro, honor, reputación, vida privada, configuración y aspectos físicos, o bien en la consideración que de ella tienen los demás, lo hace consistir en una lesión a los conceptos enumerados y obliga al responsable a repararlo mediante una indemnización pecuniaria. Aunado a lo anterior, y si se tiene en cuenta que jurídicamente es posible que además de las personas físicas, las morales también sean sujetos de derechos y obligaciones, según los artículos 25 a 27 del mencionado código, las cuales adquieren personalidad para realizar ciertos fines distintos a los de cada uno de los miembros que las componen, como lo establece el artículo 2o. de la Ley General de Sociedades Mercantiles; que obran y se obligan por medio de los órganos que las representan, y si el derecho les atribuye la calidad de personas morales a esas colectividades que adquieren unidad y cohesión a través de la personalidad, y por medio de esta construcción técnica les permite adquirir individualidad de manera similar al ser humano, y toda vez que el daño moral está íntimamente relacionado con los derechos de la personalidad, es indudable que por equiparación y analogía los conceptos relativos a la reputación y a la consideración que de sí misma tienen los demás, también se aplican a las personas morales.* Contradicción de tesis 100/2003-PS. Entre las sustentadas por los Tribunales Colegiados Octavo y Décimo Tercero, ambos en Materia Civil del Primer Circuito. 1o. de diciembre de 2004. Cinco votos. Ponente: Juan N. Silva Meza. Secretario: Manuel González Díaz. Tesis de jurisprudencia 6/2005. Aprobada por la Primera Sala de este Alto Tribunal, en sesión de fecha veintiséis de enero de dos mil cinco.

utilizarlos o revelarlos sólo con el consentimiento de la persona a quien correspondan³⁰⁶.

La Corte ha dejado claro que el derecho a la protección de datos personales corresponde solo a las personas físicas y no a las morales. Esto es así, por estar encausado al respeto de un derecho personalísimo como es el de la intimidad, señalando que de esta última ha derivado el derecho a la protección de datos. Asimismo, establece que el derecho a la privacidad corresponde únicamente a las personas físicas³⁰⁷. La Sentencia precisa a la letra lo siguiente:

³⁰⁶ ACTO DE MOLESTIA. LO CONSTITUYE LA TOMA DE FOTOGRAFÍAS A QUIENES NO TIENEN LA CALIDAD DE DETENIDOS O PRESUNTOS RESPONSABLES. La toma de fotografías a personas que no han sido puestas a disposición del Ministerio Público en calidad de detenidas o presuntas responsables -cuando éste sólo ha ordenado su localización y presentación- configura un acto de molestia porque menoscaba o restringe derechos de la persona, al hacer uso de su imagen, aunado a que la obtención de fotografías puede resultar violatoria de los derechos a la honra y a la dignidad contenidos en los artículos 17 del Pacto Internacional de Derechos Civiles y Políticos y 11 de la Convención Americana sobre Derechos Humanos, si el Estado incumple con sus obligaciones relativas a la protección de datos personales, las cuales consisten en: a) solicitar o registrar información que contenga datos personales sólo en los casos previstos por la ley; y, b) tratar confidencialmente tales datos, lo que implica utilizarlos o revelarlos sólo con el consentimiento de la persona a quien correspondan. Así, el hecho de que la autoridad obtenga fotografías de cualquier persona, sin importar su situación jurídica, efectivamente representa un menoscabo y un deterioro en sus derechos, de naturaleza continuada, pues mientras el resultado del acto (las fotografías) no se elimine, el acto de molestia continúa. Amparo directo 9/2008. 12 de agosto de 2009. Mayoría de cuatro votos. Disidente: Sergio A. Valls Hernández. Ponente: José Ramón Cossío Díaz. Secretario: Miguel Enrique Sánchez Frías. Registro No. 166037. Localización: Novena Época. Instancia: Primera Sala. Fuente: Semanario Judicial de la Federación y su Gaceta. XXX, Noviembre de 2009. Página: 401. Tesis: 1a. CLXXXVIII/2009. Tesis Aislada. Materia(s): Penal.

³⁰⁷ TRANSPARENCIA Y ACCESO A LA INFORMACIÓN PÚBLICA GUBERNAMENTAL. LOS ARTÍCULOS 3o., FRACCIÓN II, Y 18, FRACCIÓN II, DE LA LEY FEDERAL RELATIVA, NO VIOLAN LA GARANTÍA DE IGUALDAD, AL TUTELAR EL DERECHO A LA PROTECCIÓN DE DATOS PERSONALES SÓLO DE LAS PERSONAS FÍSICAS. Si se toma en cuenta que la garantía constitucional indicada no implica que todos los sujetos de la norma siempre se encuentren en condiciones de absoluta igualdad, sino que gozan de una igualdad jurídica traducida en la seguridad de no tener que soportar un perjuicio (o privarse de un beneficio) desigual e injustificado, se concluye que los artículos 3o., fracción II, y 18, fracción II, de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental, al tutelar sólo el derecho a la protección de datos personales de las personas físicas y no de las morales, colectivas o jurídicas privadas, no violan la indicada garantía contenida en el artículo 1o. de la Constitución Política de los Estados Unidos Mexicanos, pues tal distinción se justifica porque el derecho a la protección de los datos personales se refiere únicamente a las personas físicas por estar encausado al respeto de un derecho personalísimo, como es el de la intimidad, del cual derivó aquél. Esto es, en el apuntado supuesto no se actualiza una igualdad jurídica entre las personas físicas y las morales porque ambas están en situaciones de derecho dispares, ya que la protección de datos personales, entre ellos el del patrimonio y su confidencialidad, es una derivación del derecho a la intimidad, del cual únicamente goza el individuo, entendido como la persona humana. Amparo en revisión 191/2008. Grupo Senda Autotransporte, S.A. de C.V. 7 de mayo de 2008. Cinco votos. Ponente: José Fernando Franco González Salas. Secretario: Óscar Rodríguez Álvarez. Registro No. 169167. Localización: Novena Época. Instancia: Segunda Sala.

“Esto es, en el apuntado supuesto no se actualiza una igualdad jurídica entre las personas físicas y las morales porque ambas están en situaciones de derecho dispares, ya que la protección de datos personales, entre ellos el del patrimonio y su confidencialidad, es una derivación del derecho a la intimidad, del cual únicamente goza el individuo, entendido como la persona humana”.

Posteriormente, con relación a la transparencia judicial, en un criterio de 2006 la SCJN establece que con el fin de respetar el derecho a la protección de datos personales, al hacerse públicas las sentencias, se omitirán los datos de los individuos cuando manifiesten su oposición de manera expresa. Asimismo impuso a los órganos jurisdiccionales federales la obligación de que en el primer acuerdo que dicten en los asuntos de su competencia, señalen a las partes el derecho que les asiste para oponerse, en relación con terceros, a esa publicación, entendiendo que la falta de oposición conlleva su consentimiento para que la sentencia respectiva se publique sin supresión de datos.

Esta tesis además señala que la protección de los datos personales es un derecho para las personas físicas, pues así lo señala la fracción II del artículo 3 LAI, al indicar que por aquellos debe entenderse la información concerniente a una persona física identificada o identificable, excluyendo así a las personas morales, entre las que se encuentran las autoridades responsables³⁰⁸.

Fuente: Semanario Judicial de la Federación y su Gaceta. XXVIII, Julio de 2008. Página: 549. Tesis: 2a. XCIX/2008. Tesis Aislada. Materia(s): Administrativa, Constitucional.

³⁰⁸ TRANSPARENCIA Y ACCESO A LA INFORMACIÓN PÚBLICA GUBERNAMENTAL. LA CONFIDENCIALIDAD DE LOS DATOS PERSONALES SÓLO CONSTITUYE UN DERECHO PARA LAS PERSONAS FÍSICAS MAS NO DE LAS MORALES (AUTORIDADES RESPONSABLES). De la interpretación sistemática de los artículos 1, 3, 4, 8, 18 a 22 y 61 de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental, en relación con el Acuerdo General 76/2003, del Pleno del Consejo de la Judicatura Federal, que modifica los artículos 19 y tercero transitorio del Acuerdo General 30/2003, que establece los órganos, criterios y procedimientos institucionales para la transparencia y acceso a la información pública para ese órgano del Poder Judicial de la Federación, los Tribunales de Circuito y los Juzgados de Distrito, se advierte que entre los objetivos de la ley citada se encuentra el garantizar la protección de los datos personales en posesión de los sujetos obligados, es decir, la información concerniente a una persona física, identificada o identificable, y para lograrlo otorgó facultades al Pleno del Consejo de la Judicatura Federal, el que dictó los acuerdos correspondientes, estableciendo en relación con los datos personales de las partes, que con el fin de respetar cabalmente tal derecho, al hacerse públicas las sentencias, se omitirán cuando manifiesten su oposición de manera expresa, e impuso a los órganos jurisdiccionales la obligación de que en el primer acuerdo que dicten en los asuntos de su competencia, señalen a las partes el derecho que les asiste para oponerse, en relación con terceros, a esa publicación, en la inteligencia de que la falta de oposición conlleva su consentimiento para

13. Tendencias

En la actualidad, el derecho a la protección de datos personales ha adquirido una importancia que desde su surgimiento se veía venir; así como, los retos que representaría su evolución a la par de las nuevas tecnologías y medios de comunicación, para satisfacer las necesidades de protección de la privacidad de las personas.

Este apartado sobre “Tendencias”, no es exclusivo de México, sin embargo, es indexado en este capítulo por considerarlo el más adecuado, ya que los países europeos están o han trabajado con estos asuntos. El Estado mexicano, por su parte, deberá ser consciente en que la emisión de la nueva normativa en protección de datos, no da por concluido el tema; sino que, solamente marca un parteaguas en la materia para continuar por el camino de su estudio y regulación.

13.1 Internet y las redes sociales

El avance de la tecnología ha impulsado lo que hoy se conoce como la *sociedad de la información*, cuyos servicios cubren también aquellos consistentes en transmitir datos a través de una red de comunicación o albergar información facilitada por el destino del servicio (Del Peso Navarro, 2003: 8)³⁰⁹, en otras

que la sentencia respectiva se publique sin supresión de datos; de donde se concluye que la protección de los datos personales de referencia sólo constituye un derecho para las personas físicas, pues así lo señala la fracción II del artículo 3 de la ley mencionada, al indicar que por aquéllos debe entenderse la información concerniente a una persona física identificada o identificable, excluyendo así a las personas morales, entre las que se encuentran las autoridades responsables. TERCER TRIBUNAL COLEGIADO DEL DÉCIMO TERCER CIRCUITO. Amparo en revisión 550/2004. Tesorería de la Federación y otras. 21 de enero de 2005. Unanimidad de votos. Ponente: Robustiano Ruiz Martínez. Secretaria: Elena Elvia Velasco Ríos. Reclamación 12/2005. Director Regional de Vigilancia de Fondos y Valores de la Tesorería de la Federación. 12 de septiembre de 2005. Unanimidad de votos. Ponente: Robustiano Ruiz Martínez. Secretaria: Elena Elvia Velasco Ríos. Nota: El Acuerdo General 30/2003 citado, aparece publicado en el Semanario Judicial de la Federación y su Gaceta, Novena Época, Tomo XVIII, noviembre de 2003, página 1065. Registro No. 176077. Localización: Novena Época. Instancia: Tribunales Colegiados de Circuito. Fuente: Semanario Judicial de la Federación y su Gaceta. XXIII, Enero de 2006. Página: 2518. Tesis: XIII.3o.12 A. Tesis Aislada. Materia(s): Administrativa.

³⁰⁹ *Internet* se ha resistido a ser controlado por organizaciones gubernamentales de cualquier clase. El modelo estatalista no ha podido ser transportado a la gran red. La *domestic analogy* ha sido rechazada como opción organizativa. La autonomía de *Internet* es, en la actualidad, una realidad incontestable y su independencia ha sido mantenida a ultranza y contra la corriente de las tendencias regulatorias establecidas a escala mundial para otras tecnologías de la comunicación (Muñoz Machado, 2010: 82).

palabras, la transferencia que se hace al proporcionar datos personales para un determinado fin o uso.

A. Internet

En nuestros días la red de comunicación más importante es *Internet*, la cual por el desarrollo y crecimiento que ha tenido en las últimas décadas, cuenta con una limitada regulación normativa de protección para el usuario. Cuando dicha red tuvo su expansión a la población es que surgió el término del *Derecho Informático o Derecho de la informática* que a decir de Pérez Luño (1996: 18) es “una materia inequívocamente jurídica, conformada por el sector normativo de los sistemas jurídicos contemporáneos integrado por el conjunto de disposiciones dirigido a la regulación de las nuevas tecnologías de la información y la comunicación, es decir, la informática y la telemática. Las fuentes y estructura telemática del Derecho informático afectan a las ramas del Derecho tradicionales. Así, se inscriben en el ámbito del Derecho público el problema de la regulación del flujo internacional de datos informáticos, que interesa al Derecho internacional público; la libertad informática, o defensa de las libertades frente a eventuales agresiones perpetradas por las tecnologías de la información y la comunicación, objeto de especial atención por parte del Derecho Constitucional y Administrativo; o de los delitos informáticos, que tienden a configurar un ámbito propio en el Derecho penal actual. Mientras que inciden directamente en el Derecho privado cuestiones tales como: los contratos informáticos, que pueden afectar lo mismo al *hardware* que al *software*, dando lugar a una rica tipología comercial en al que pueden distinguirse contratos”. Lo anterior ha dado lugar al debate, de si se trata de una nueva rama del Derecho o una nueva variante de tipología en cada una de las ya existentes.

Las violaciones a la esfera privada del individuo son frecuentes, ya que se realizan por medio de la autopista de la información, también llamada “infopista” (Del Peso Navarro y Ramos González, 2002: XXXV). La navegación en la red implica la generación de una serie de datos de carácter personal del usuario y su captación por los diferentes sujetos que intervienen, en mayor o menor medida según sus funciones (Messía de la Cerda Ballesteros, 2004: 101).

No es posible ocultar cómo *Internet* cambia la cultura de los países, llegando incluso a homogeneizarla, por ello, es apremiante una regulación de la materia que sea específica y además eficaz. Tal telaraña universal condensa a la perfección el horizonte digital, junto a las últimas tendencias en el tránsito electrónico, erigiéndose así en la máxima expresión de las nuevas tecnologías (Ballesteros Moffa, 2005: 108-109).

Así que, *Internet* hoy se ha convertido en sinónimo de comunicación que –generalmente y de forma gratuita- ofrece una amplia gama en métodos de comunicación y transferencia de información, por ejemplo: el correo electrónico, chats, páginas webs, blogs, foros de discusión, redes sociales, etc.³¹⁰. Estas últimas, a la par de las múltiples ventajas que presentan, han venido ocasionando una serie de problemas graves para la intimidad del ser humano, dado que *Internet* y su programación innovadora se mantienen siempre lejos de la previsión normativa que el legislador pueda realizar.

B. Redes sociales

Una red social es aquella estructura de personas o grupos de individuos³¹¹, que comparten intereses de diversa índole (académicos, profesionales, religiosos, políticos, deportivos, etc.) o que guardan alguna relación entre sí producto de sus intereses, hábitos, relaciones familiares, costumbres, etc., cuyo objetivo es el fortalecimiento de los lazos personales y profesionales entre sus socios y otros grupos, en función del interés que los une y comparten, así como la difusión de éste.

Actualmente, las redes sociales se pueden agrupar en tres clases según su forma de interactuar:

1. Convencionales: aquellas que surgen por el método clásico de reunión y no utilizan los recursos proporcionados por las nuevas tecnologías, como consecuencia del escaso desarrollo informático del país sede y la disponibilidad de *Internet* a la población, o bien por decisión propia.

³¹⁰ Con relación al efecto de internet en la actualidad véase a Kagan (2010: 240-241).

³¹¹ Asociaciones, organizaciones, fundaciones, congregaciones, etc.

2. Modernas: también llamadas “redes sociales en *Internet*”. Surgen a través de *Internet* y la interacción de sus miembros se realiza a través de este medio. Así tenemos redes tales como Facebook, Google+, Twitter, Tuenti, MySpace, entre otras.
3. Mixtas: surgen de forma convencional o moderna y la interacción de sus miembros se realiza de ambas formas simultáneamente.

a. Red social convencional

Esta clase se sitúa antes del uso habitual de *Internet*, en donde el modo de socializar de sus usuarios es de forma presencial. Este tipo de red social se desenvuelve en el campo del trato directo y el uso de los medios de comunicación ordinarios.

Las ventajas son principalmente el trato directo y lo que ello conlleva como el uso del lenguaje en lo que hace a entonación y modulación de la voz, gestos corporales, trato personal, educación, buenas maneras, entre otras. Por su parte, las desventajas son varias, entre las que se pueden destacar que: a) La comunicación es lenta por el uso de los medios de comunicación convencionales; b) El número de integrantes se ve limitado a personas que se circunscriban a una determinada área geográfica; y c) Los horarios de actividad se limitan a tiempos de participación preestablecidos.

b. Red social en Internet

En la actualidad ha surgido una nueva variante de la tradicional red social, es decir, aquellas cuyo campo de interacción se desenvuelve dentro de la gran red. Las primeras redes sociales en *Internet* surgen aproximadamente a partir del año 2002, pero es hasta el 2006 en que éstas se popularizan por el lanzamiento público de la red social denominada *Facebook*. Es entonces, en que la forma de interactuar de las personas ha cambiado.

Los cambios son sustanciales ya que los individuos han perdido interés en la relación personal directa con las personas y se han volcado dentro de la vida digital. Las ventajas de esta clase de red son muchas y muy variadas, por

ejemplo: a) La comunicación inmediata, ágil y eficaz; b) El número de integrantes puede llegar a ser muy numeroso ya que no existe límite geográfico; c) Los horarios de actividad son flexibles; d) La participación es altamente fluida porque se puede realizar desde cualquier sitio y a cualquier hora a través de *Internet*.

Durante el año 2008 la 30ª Conferencia internacional de Autoridades de Protección de Datos y privacidad, adoptó la Resolución sobre Protección de la privacidad en los servicios de redes sociales³¹², cuyos puntos consisten en recomendaciones para:

Usuarios de servicios de redes sociales

1. Publicidad de la información.
2. Privacidad de otros usuarios.

Proveedores de servicios de redes sociales

1. Normas y reglamentos sobre privacidad.
2. Información sobre usuarios.
3. Control de usuarios.
4. Configuraciones por defecto que sean respetuosas con la privacidad.
5. Seguridad.
6. Derechos de acceso.
7. Eliminación de perfiles de usuario.
8. Uso del servicio bajo un seudónimo.
9. Acceso de terceros.
10. Indexación de perfiles de usuarios.

³¹² Véase:

http://www.agpd.es/portalwebAGPD/canaldocumentacion/conferencias/common/pdfs/30_conferencia_internacional/resolucion_redes_sociales.pdf (Consulta: 09/11/2012).

13.2 Riesgos y problemas actuales en Internet

Las nuevas tecnologías e Internet han desarrollado grandes riesgos para las personas, directamente relacionados a la vulneración del derecho a la protección de datos personales. Fioriglio (2008: 47-50) refiere que las amenazas se incrementan cuando el sujeto no posee el control de sus datos y la transferencia de información (imágenes, fotos, audio, etc.) por la red es cada vez mayor.

Actualmente los peligros principales son los siguientes:

A. Suplantación de la identidad

El uso de las redes sociales y la falta de regulación normativa ha traído como consecuencia, principalmente entre los adolescentes, que les sea fácil de realizar una suplantación o robo de identidad de gente a la que conocen a la cual no le guardan especial simpatía, así como de ser víctimas de ello.

B. Derecho al olvido

El derecho al olvido es un tema reciente que aún está en discusión. Se invoca por parte del sujeto que después de haber tenido sus quince minutos de fama por un mal episodio, que se olvida pero no definitivamente, ya que después resucita al estar disponible en algún medio de comunicación (Pino, 2006: 263). Actualmente, esto es muy común porque todo permanece en los motores de búsqueda de Internet.

Este derecho ha sido estudiado por la Agencia Española de Protección de Datos, por consecuencia de los buscadores en *Internet* que indexan los periódicos y Boletines Oficiales. Situación que ha ocasionado un malestar generalizado en quienes no habiendo introducido sus datos en la gran red aparecen años después como infractores administrativos o a través de una nota dedicada a despertar el morbo de los lectores de algún periódico o revista. Entre las que podemos encontrar noticias de violencia de género, infracciones propias de errores de juventud, etc.

C. Pérdida de información

El uso de los nuevos dispositivos móviles (telefonía celular, *ipads*, *e-books*, portátiles, etc.), además de la comodidad que significan en las tareas diarias, tienen un problema particular, que es el ocasionado del extravío o robo del dispositivo que es capaz de almacenar una gran cantidad de información personal como son: claves de correo electrónico y redes sociales, cuentas bancarias, información en el disco duro, agenda de contactos, fotografías, etc.

13.3 Niños y adolescentes

El grupo de mujeres, niños y adolescentes, principalmente estos últimos, son el más vulnerable a los riesgos que conduce el uso desinformado de *Internet* y sus redes sociales, debido a que proporcionan una gran cantidad de datos personales de sí mismos y de las personas que les rodean (familia, compañeros de clase, amigos, vecinos, etc.).

Esta generación de menores, son los llamados nativos de *Internet*, es decir, aquellos que nacieron cuando ya se utilizaba esta tecnología de forma habitual, manipulándola de modo tan natural que no imaginan la vida sin este medio de comunicación³¹³. Situación que ligada a la limitada efectividad de la legislación provoca que sean víctimas constantes de amenazas informáticas y de personas que les acechan. En este sentido, no es raro que los problemas y delitos que existían en la vida física hayan evolucionado al campo informático, es así que hoy existen los términos de *ciberbullying*, *grooming* y *sexting*.

³¹³ Piñar Mañas (2011: 62-68) a este respecto, refiere de una manera por demás ilustrativa el hecho de que los adultos viven “con” internet, mientras que los menores viven “en” internet. Por lo tanto, ellos no se planetan que su realidad virtual salga más allá de su propio espacio en la red social y sus amigos. Por su parte, Murillo de la Cueva (2011: 109) refiere que las situaciones jurídicas que provocan el fenómeno de la actividad de los menores en internet ocasionan conflictos de competencia en la resolución de tales casos, por un lado están los mecanismos locales y por otro los regiones o internacionales, por lo que en ocasiones puede no haber coherencia entre ambos.

A. *Cyberbullying*

Los expertos han elaborado un concepto nuevo de violencia que se vale de medios electrónicos y que recibe el nombre de *cyberbullying* o ciberacoso³¹⁴. Esta conducta se define como acoso entre iguales en el entorno de las nuevas tecnologías de la información y la comunicación (TIC), e incluye actuaciones de chantaje, vejaciones e insultos de niños a otros niños. En una definición más exhaustiva, se puede decir que el *cyberbullying* supone el uso y difusión de información lesiva o difamatoria en formato electrónico a través de medios de comunicación como el correo electrónico, la mensajería instantánea, las redes sociales, la mensajería de texto a través de teléfonos o dispositivos móviles o la publicación de vídeos y fotografías en plataformas electrónicas de difusión de contenidos. La clave, en cualquier caso, es que se trata de una situación en que acosador y víctima son niños: compañeros de colegio o instituto y personas con las que se relacionan en la vida física (INTECO, 2009: 3).

En España el *cyberbullying* es el descrito con anterioridad, pero en Estados Unidos, este nuevo término tiene un significado de intimidación virtual, es decir, utilizando internet para enviar o publicar mensajes hirientes. Así, el uso de la tecnología es empleado para controlar e intimidar a otras personas del centro educativo, ya que este tema hace referencia principalmente a los compañeros de clase, por ser con quienes el menor convive la mayor parte del tiempo. Sin embargo, es importante aclarar que también podría tratarse de compañeros del club deportivo del niño u otros centros de actividades en los que se desenvuelva. Las intimidaciones a través de internet, también pueden ser en contra de adultos como profesores o personal administrativo, sin embargo, cuando un adulto es el objetivo esto es definido como *cyberharrassment*.

La intimidación es un arma poderosa de opresión durante la escuela secundaria y la preparatoria (bachillerato), cuando los estudiantes forman grupos o camaraderías que tienen como base intereses, valores, habilidades y gustos a fin de ganar la aceptación y el sentimiento de pertenencia que les proporciona

³¹⁴ Aquí se pueden apreciar dos elementos que más adelante reflexionaremos. El término real en inglés es “*cyberbullying*”, al castellanizar esta palabra se ha hecho incluso con un error ortográfico del idioma original, además de traducirla como ciberacoso, lo que es discutible.

seguridad. Pertener e identificarse con un grupo es saludable para la realización personal, sin embargo, este mismo sistema de identificación con un grupo crea una cultura que nutre la discriminación mediante la exclusividad y la exclusión³¹⁵ (Moy, 2010: 566).

El *bullying* es un término inglés que se traduce en intimidación, mientras que el *harrassment* significa acoso. Ambas acciones, cuando son llevadas a cabo mediante el uso de la tecnología, se les antepone el prefijo *cyber* dando lugar a los términos de *cyberbullying* (ciber-intimidación) y *cyberharrassment* (ciber-acoso). Cuando se intenta castellanizar términos anglosajones, sin dar la palabra apropiada en castellano, surgen las traducciones confusas, como ahora es el caso. Según la Real Academia Española intimidar y acosar no son lo mismo:

1. **Intimidar** (*bullying*): Causar o infundir miedo. //Entrarle o acometer a alguien el miedo.
2. **Acosar** (*harrassment*): Perseguir, sin darle tregua ni reposo, a una persona. //Perseguir, apremiar, importunar a alguien con molestias o requerimientos.

En este sentido, se puede percibir que la intimidación tiene como objetivo una violencia psicológica que no necesariamente tiende a manifestarse físicamente, o que por lo menos no es la intención principal; mientras que en el acoso existe una persecución, que en el plano normal es física y cuyas molestias pueden ser variadas, en el acoso siempre aparecerá la intimidación. Normalmente, en las codificaciones penales el acoso u hostigamiento suele tener connotaciones propias de la libertad sexual, en el ámbito laboral o docente.

Por otro lado, si se habla de estas acciones en el ámbito virtual, ninguna será física ya que todo se desarrolla en el ámbito de las nuevas tecnologías. Se podría decir que la diferencia la haría la continuidad de las acciones, ya que la intimidación puede presentarse una o un par de veces, sin que sea acoso, mientras que el acoso, conlleva en si una sugerencia de continuidad y actos repetidos.

³¹⁵ La autora refiere el *bullying* o intimidación, como consciente, voluntaria y de actividad hostil cuya intención es causar daño, provocar el miedo a través de la amenaza de la agresión y crear temor.

La legislación penal es la apropiada para definir la intimidación y el acoso, por ello no ahondaremos más. Y para concluir con este epígrafe se ha de concluir, que actualmente el *cyberbullying*, es el acoso entre menores, mientras que el *cyberharrassment* es cuando el objetivo es un adulto. Y ambos, pueden ser constitutivo de un abanico de delitos como: amenazas, coacciones, injurias y calumnias, que se pueden transformar en agresiones.

B. Grooming

Esta es otra situación que puede implicar un riesgo para la seguridad e integridad de los menores. Se trata del acoso ejercido por un adulto y se refiere a las acciones realizadas deliberadamente para establecer una relación y un control emocional sobre un niño o niña con el fin de preparar el terreno para el abuso sexual del menor. Se podría decir que son situaciones de acoso con un contenido sexual explícito o implícito (INTECO, 2009: 4).

Internet ha venido contribuir al anonimato de los agresores a menores como pedófilos y pederastas (Marcoccia, 2006: 363-367), ya que es a través de la web que estos buscan a sus víctimas, quienes dado que están bastante tiempo en internet socializando y sin una adecuada orientación al respecto, no es difícil que se vean afectadas por diversos peligros.

El *grooming* puede ser constitutivo de un abanico de delitos como: exhibicionismo, difusión de contenido pornográfico y corrupción de menores.

C. Sexting

El *sexting* consiste en la difusión o publicación de contenidos (principalmente fotografías y videos) de tipo sexual, producidos por el propio remitente, utilizando para ello el teléfono móvil u otro dispositivo tecnológico³¹⁶. En Estados Unidos, en la franja de edad de 13 a 18 años, son más chicas (65%) que chicos (35%) los que envían *sexting* a través de SMS o *e-mails* (INTECO, 2011: 4).

³¹⁶ Imaginemos que los destinatarios a su vez la renvían a otros, es a partir de aquí, puede entrar en un proceso de renvío masivo multiplicándose su difusión.

Sexting es una palabra proveniente del inglés que une “*sex*” (sexo) y “*texting*” (envío de mensajes de texto vía SMS desde teléfonos móviles). Aunque el sentido original se limitara al envío de textos, el desarrollo de la telefonía móvil ha llevado a que actualmente este término se aplique al envío, especialmente a través del teléfono móvil, de fotografías y videos con contenido de cierto nivel sexual, tomadas o grabados por el protagonista de los mismos (INTECO, 2011: 6).

Relacionado con el *sexting* se encuentra el llamado *sex-casting*. Con este término se identifica la grabación de contenidos sexuales a través de la *webcam* y difusión de los mismos por e-mail, redes sociales o cualquier canal que permitan las nuevas tecnologías.

V. Conclusiones

El derecho a la protección de datos personales es un claro producto de la época actual en torno a la evolución de las nuevas tecnologías. Esta tesis se ha enfocado en analizar las principales características y diferencias que éste hubo de adoptar para el caso español y mexicano. En este sentido, el trabajo destacó los principales elementos de carácter histórico que han determinado la configuración de este derecho hasta nuestros días.

La presente investigación se estructuró en función de cuatro apartados, todos importantes para una adecuada comprensión del tema, iniciando por las generalidades del origen del derecho a la protección de datos personales, continuando con las primeras inserciones constitucionales en el mundo de este nuevo derecho, después abordando el tema sobre el caso español que ha sido el principal referente en México y concluyendo con la situación actual del Estado mexicano y de su reciente legislación en este ámbito. Y con este trayecto, se han llegado a las siguientes reflexiones:

1. Autonomía del derecho fundamental a la protección de datos personales en cuanto a su definición, pero de difícil emancipación práctica al momento de su ejercicio con relación a la privacidad.

Estamos de acuerdo en que es un derecho que goza de autonomía propia, en lo que hace a su definición y delimitación jurisprudencial, aunque en la práctica sigue estando íntimamente ligado con el derecho a la privacidad. Lo anterior es así, porque al ejercitar el derecho a la protección de datos personales, se estará eventualmente salvaguardando también el derecho a la privacidad, en alguna de sus facetas.

No obstante lo anterior, el derecho a la protección de datos se constituye como un derecho independiente que responde a necesidades diversas –respecto del derecho a la privacidad–, que van desde el inadecuado tratamiento manual de los datos personales por quienes poseen la información, hasta verdaderos peligros que surgen de los diversos métodos de automatización de procedimientos y fugas de información personal de los individuos. La STC 292/2000 hubo de diferenciar

la intimidad del derecho a la protección de datos en lo que hace a su función, objeto y contenido.

2. Existe una útil delimitación jurisprudencial del Tribunal Constitucional español del derecho a la protección de datos personales atendiendo a la función, objeto y contenido, que ayuda a diferenciarlo del derecho a la intimidad.

En lo que hace a la delimitación del derecho a la protección de datos respecto de la intimidad, estamos de acuerdo con la proporcionada por el Tribunal Constitucional español en su Sentencia 292/2000. En cuanto a su “*función*”, precisa que el *derecho a la intimidad* protege al individuo frente a cualquier invasión que pueda realizarse en el ámbito de la vida personal y familiar, es decir, el poder de resguardar su vida privada de una publicidad no deseada. Mientras que, el *derecho de protección de datos*, persigue garantizar a la persona, un poder de control sobre sus datos personales, su uso y destino, con el propósito de impedir su tráfico ilícito y lesivo para la dignidad y derecho del afectado. Este derecho garantiza a los individuos un poder de disposición sobre esos datos.

Por lo que hace al “*objeto*” de ambos derechos la singularidad del derecho a la protección de datos, es un objeto más amplio, comparado con el derecho a la intimidad. El derecho a la *protección de datos* amplía la garantía constitucional a aquellos datos que sean relevantes o tengan incidencia en el ejercicio de cualesquiera derechos de la persona, sean o no derechos constitucionales y sean o no relativos al honor, la ideología, la intimidad personal y familiar, y a cualquier otro bien constitucionalmente amparado. El objeto de protección también alcanza a aquellos datos personales públicos, que no escapan al poder de disposición del afectado porque así lo garantiza su derecho a la protección de datos. También por ello, el que los datos sean de carácter personal no significa que sólo tengan protección los relativos a la vida privada o íntima de la persona, sino que los datos amparados son todos aquellos que identifiquen o permitan la identificación de la persona, pudiendo servir para la confección de algún perfil de la personalidad.

En cuanto al distinto “*contenido*” de ambos derechos, la Sentencia precisa que el derecho a la intimidad personal y familiar, confiere a la persona el poder jurídico de imponer a terceros el deber de abstenerse de toda intromisión en la esfera íntima de la persona y la prohibición de hacer uso de lo así conocido. Mientras que el derecho a la protección de datos atribuye a su titular un haz de facultades consistente en diversos poderes jurídicos cuyo ejercicio impone a terceros deberes jurídicos, asimismo garantiza a la persona un poder de control y disposición sobre sus datos personales, lo que sólo es posible y efectivo imponiendo a terceros los mencionados deberes de hacer a fin de cumplir con los derechos del titular que son: el derecho a que se requiera el previo consentimiento para la recogida y uso de los datos personales, el derecho a saber y ser informado sobre el destino y uso de esos datos y el derecho a acceder, rectificar y cancelar dichos datos. En definitiva, el poder de disposición sobre los datos personales.

3. Necesidad de estandarizar la normativa a nivel internacional para que se refleje en el ámbito nacional.

En la actualidad, debido a la instantaneidad y ubicuidad de la sociedad en la era de la globalización, el comportamiento de los individuos ha tendido a homogenizarse culturalmente. Asimismo, la solución a las necesidades y la expansión de los problemas que las nuevas tecnologías han traído consigo. Por ejemplo, el *cloud computing* o cómputo en la nube, que es una nueva manera de almacenar datos, lo que conlleva nuevos escenarios en el tratamiento, transmisión y manejo de información, lo que ha dificultado el cumplimiento de la normativa actual de cada país. Por ello, la regulación legal del tema, es una necesidad cuya solución está pendiente, así como el impulso de una legislación internacional estándar que logre agrupar lo mejor de todos los instrumentos que actualmente existen.

4. El derecho a la protección de datos personales podría presentar colisión con otros derechos fundamentales, la que se deberá resolver mediante la ponderación adecuada para cada caso.

El camino por el cual ha transitado la configuración de este derecho no ha sido rápido, ni ha surgido por espontaneidad. Por el contrario, lo ha hecho

lentamente. Concretamente, ha atendido a la necesidad de las personas de tener el control de su propia información personal, para convertirse en un medio más para velar de otros derechos fundamentales, tales como la dignidad, privacidad, propia imagen, honor, vida, información, etc.

En este sentido, el derecho a la protección de datos personales puede presentar colisión con el derecho a la información, situación que únicamente puede ser resuelta atendiendo a una adecuada ponderación de derechos. Sin embargo, en la actividad de los órganos de la Administración Pública, habrá de primar la máxima transparencia debido al origen de sus ingresos a partir de los impuestos gravados al ciudadano, salvo por las restricciones que la ley precise. Asimismo, se ha de señalar que habrá otros casos en los que se tendrá que hacer una correcta ponderación de ambos derechos atendiendo al caso particular, en cuanto al interés público y al grado de afectación al titular de la información. En México, y como se desprende de la Resolución 932/2005 de 11 de junio emitida por el IFAI (adjunta en los anexos de este trabajo), se ha avanzado desde hace años en la publicidad de la remuneración de los servidores públicos porque provienen de la contribución ciudadana, y sería un retroceso que a partir de la introducción de este derecho en México se llegará a sostener en algún momento, que dicha información es un dato personal de carácter patrimonial y por ende no susceptible de revelar.

5. En relación con España, México presenta un desfase de casi dos décadas, que lo hace vulnerable en esta era de globalización y cambio estructural de la sociedad.

Actualmente, la sociedad se encuentra en un cambio estructural que transcurre en la era de la globalización y las nuevas tecnologías, que relaciona a todos los individuos entre sí, en función de diversos roles. Por ello, la información que fluye en dichas interacciones debe preservar derechos de la persona como la privacidad y la protección de datos personales.

En este sentido, y como se deduce del análisis de los sistemas jurídicos español y mexicano, en materia de protección de datos, no ha sido una constante comparación en paralelo, dado que el surgimiento del derecho no se presenta en

una misma línea temporal. México, respecto de España, presenta un desfase de 18 años desde la publicación de la primera normativa española de protección de datos de 1992 (LORTAD) –la posterior y actualmente vigente es la LOPD de 1999- hasta la Ley mexicana de 2010. Esta situación convierte al país en vulnerable ya que el estado mexicano está en un proceso de implementación y adecuación de la normativa, así como de concientización de la población. La vulnerabilidad también se presenta en cuanto a la ausencia de una adecuada delimitación judicial y jurisprudencial del derecho, lo que no es de extrañar dada su reciente incorporación al ordenamiento jurídico.

6. Hay un primer surgimiento del derecho a la protección de datos personales en México, que fue poco eficaz y limitado en su ejercicio y garantía en 2002.

El derecho a la protección de datos personales en México aparece por primera vez en el año 2002 en la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental. Después, con las reformas constitucionales de 2009, de los artículos 16 y 73 de la Constitución. Evolución legislativa que concluye, recientemente, con la publicación de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (2010), y de su Reglamento (2011). Este primer surgimiento fue poco eficaz, ya que entonces, solamente se refería en la Ley de Transparencia la protección de datos personales en posesión de la administración pública y no aquellos en posesión de particulares, como ocurre actualmente.

Dicho sea de paso, que además esta escueta regulación del derecho a la protección de datos se asoma en el 2002 que es cuando aparece en México la Ley de Transparencia. Así entonces, y dada la historia del país en temas de corrupción, el esfuerzo se condujo hacia objeto principal de dicha Ley, es decir, la transparencia y el acceso a la información pública; no se desarrollándose adecuadamente el derecho a la protección de datos personales. Hoy en día, el derecho a la transparencia se encuentra en una etapa de madurez, y las necesidades de la sociedad actual requieren además de la consolidación del

derecho a la protección de datos personales, a fin de tener el poder de disposición de su propia información.

7. La Ley española de protección de datos es fuente inspiradora de la actual norma mexicana.

Producto de los vínculos históricos y de cooperación con España, de la lectura de la Ley mexicana se desprende la marcada influencia que ha tenido la experiencia española, y los principales temas de discusión en la actualidad entre los especialistas, derivados de la realidad tecnológica del momento como por ejemplo el *cloud computing* en el art. 52 RLOPD, que es una nueva forma de almacenar información y cuya regulación no es fácil, por no haber una legislación internacional estándar. Así como, la aclaración del derecho de oposición en la Ley (arts. 8 y 27 LPDP), omisión que en Ley española ha dado lugar a alguna crítica (arts. 34 a 36 RLOPD), y que en la mexicana es una clara rectificación.

España ha evolucionado en este derecho gracias a la práctica en otras latitudes europeas. Este proceso se ha nutrido no solo de la aportación de la distinta normatividad en Europa, sino también del trabajo de la Agencia Española de Protección de Datos y de sus homólogas autonómicas, así como por la doctrina emitida del Tribunal Constitucional. De esta manera, hoy se tiene definida la estructura, límites y contenido del derecho. Esta experiencia ha permeado en Latinoamérica y ha contribuido en los trabajos de legislación existente en la materia.

8. Urge la difusión del derecho a la protección de datos personales a la población de una forma clara, continua, seria y comprometida por parte de la autoridad.

Hoy México reconoce la importancia del derecho fundamental a la protección de datos personales. Aunque tardíamente cuenta con una Ley especializada y su Reglamento. Por lo tanto, es urgente la actuación de los titulares del derecho en la exigencia del respeto al mismo. Sin embargo, el ejercicio de este derecho brillará por su ausencia, en tanto en cuanto, la persona no tenga conocimiento de los derechos y acciones que le asisten.

9. La configuración mexicana del aviso de privacidad ordenado por la propia Ley es una novedad.

Una de las diferencias del ordenamiento mexicano, respecto del español, es que el aviso de privacidad se encuentra regulado por la Ley y su Reglamento. Por su parte, España lo regula únicamente en el Reglamento. La Secretaría de Economía mexicana, en coadyuvancia con el Instituto, es la responsable de emitir los lineamientos correspondientes para el contenido y alcances del aviso de privacidad. Y en consecuencia, en junio de 2011 ha sido publicada la Guía práctica para generar el aviso de privacidad (que no los lineamientos), en la que orienta a los responsables del tratamiento de datos personales para la elaboración, diseño y difusión del aviso de privacidad. Esta Guía es completa y ejemplifica ampliamente los requerimientos de la Ley para el citado aviso.

10. El formato del aviso de privacidad indicado por la ley es complejo y dificulta la adaptación de la normativa.

La Guía para generar el aviso de privacidad emitida por la Secretaría de Economía, precisa que el aviso variará de longitud, siendo completo o simplificado, en función de diversos factores como: el espacio para agregar el aviso, el medio por el cual se recaba la información, el tipo de datos que se recogen y si se prevé o no una transferencia. En este último caso la autorización a la transferencia internacional se da por defecto, a no ser que, el titular se oponga a la misma marcando la casilla correspondiente. Por otro lado, cuando el aviso no contempla un espacio suficiente, remite al titular a la búsqueda del aviso completo.

Por lo anterior, no es de extrañar que el tema del aviso de privacidad, no obstante los esfuerzos por hacerlo demasiado acorde a derecho, lo han convertido en confuso. Además, hace que la remisión al documento completo, contenga un grado de poca claridad en la manifestación de la voluntad, convirtiéndose en un elemento que suscite desconfianza para el ciudadano. El aviso completo, es asimilable a un contrato corto y con cierto grado de dificultad, lo que se agrava cuando se está delante de una normativa de nueva implementación, que debería

de ser un instrumento sencillo, y totalmente contrario a una situación de poca practicidad a efectos de difusión y concientización.

11. Se percibe la necesidad de homogenizar los principios del tratamiento en la normativa mexicana de protección de datos personales del sector público y privado.

Los principios que los responsables deberán observar, cumplen con la finalidad de la necesidad actual y están acordes a los requerimientos internacionales. Sin embargo, y dado que se cuenta con una regulación diferenciada de los datos en posesión del sector público y el privado, es conveniente una adecuada unificación, a fin de que la normativa de este nuevo derecho sea más clara para el usuario. En el caso del sector público, los principios se encuentran en Lineamientos y no en un Reglamento como es el caso del sector privado.

La lista de los principios en uno y otro, no se comparten en su totalidad en lo que hace a la denominación y el contenido. Por ejemplo, aquellos que no se aprecian claramente en la regulación del sector público, y si en el privado, son los de finalidad, lealtad, proporcionalidad y responsabilidad; pero que se ven en el conjunto de la definición del principio de calidad como: exacto (lealtad), adecuado (responsabilidad), pertinente (finalidad y responsabilidad) y no excesivo (proporcionalidad, lealtad y finalidad). Por su parte, el de Seguridad que se encuentra en este apartado y cuya nomenclatura cambia en el de particulares por el de Responsabilidad, no termina por precisar el aspecto del deber de secreto.

Continuando con este tema, hay menciones importantes en los principios del sector privado, por ejemplo, el de licitud (art. 7 LPDP y art. 10 RLPDP) que se deberá observar en la recogida y en el tratamiento de los datos. Por su parte, el Reglamento a la Ley agrega que dicho tratamiento deberá hacerse atendiendo a la legislación mexicana y al derecho internacional. Esta última mención, es importante, no sólo por los instrumentos internacionales regionales que existen en Europa (que si bien no son vinculantes, si son orientativos), sino además por la existencia de una tendencia actual hacia la estandarización de la normativa del

derecho a la protección de datos personales, por lo que no es de extrañar, que en el futuro puedan surgir instrumentos reguladores de la materia.

12. El consentimiento tácito es una innovación.

En lo que hace al principio de consentimiento, se establecen dos tipos: el expreso y el tácito. Este último, a diferencia de otros países, es una novedad mexicana, y consiste en aquel que se otorga cuando habiéndose puesto a su disposición el aviso de privacidad, el titular no manifiesta su oposición. El consentimiento tácito será válido como regla general, salvo que la Ley exija el consentimiento expreso (arts. 13 y 14 RLPDP). Ahora bien, y debido a la reciente innovación de esta tipología, el reglamento no es claro en el mecanismo que se habrá de seguir en el propio aviso de privacidad, para que el titular manifieste su negativa al tratamiento.

13. Armonización del ordenamiento a nivel internacional

Por otro lado, la Ley mexicana hace mención de los esquemas de autorregulación, traducidos en códigos deontológicos o sellos de confianza. La previsión es significativa a fin de estandarizar y armonizar los tratamientos de datos, además que facilitan la labor del Instituto, mediante la colaboración en la difusión del derecho y cumplimiento de la Ley. Sin embargo, y dado que México está en un proceso de implementación de esta nueva normativa, es conveniente que el Instituto aclare detalladamente cuáles serían dichos esquemas.

14. Necesidad de un certificado que refleje un efectivo cumplimiento de la normativa de protección de datos personales en México.

De igual modo, que existen certificaciones internacionales en este ámbito, es importante crear un mecanismo similar de validez a nivel nacional, regulado por el Instituto y cuya licencia se otorgue a profesionales técnico-especializados en la materia. Lo anterior, conducirá a paso firme hacia la urgente homogenización de procesos en protección de datos. En consecuencia, se promovería el interés de la comunidad jurídica en esta área para lograr avances significativos en el cumplimiento de la LPDP, además se incentivaría la cooperación y participación internacional en este campo.

15. Necesidad de un Registro de Ficheros.

La Ley mexicana, comparada con la española, no contempla el registro de Ficheros ante la Autoridad reguladora, lo que puede representar riesgos para el individuo por parte del Responsable o encargado. Si quien recopila la información no tiene clara la Ley, ni los datos que puede tratar –lo que no es raro cuando se está en fase de implementación de una nueva normativa-, existe el peligro de crear ficheros y tratar información excesiva por no estar correctamente asesorados. La inscripción de ficheros es una medida que, en este caso, podría ser preventiva para no almacenar datos personales en una base de datos sensibles, que con posterioridad resultase ilegal.

16. Necesidad de niveles regulados de seguridad

La normativa mexicana no prevé la implementación de diferentes grados de seguridad dependiendo del tipo de datos personales a tratar. Las medidas previstas por el Reglamento pueden dar lugar a dudas, para lo cual sería importante un instrumento especial que regule distintos niveles de seguridad a cumplir por el Responsable y el encargado.

17. Necesidad de la obligación del Especialista de protección de datos.

La presencia de una persona delegada para el cumplimiento de la normativa de protección de datos en cada empresa o institución, es importante para una adecuada implementación de la Ley. Esta práctica, además incentivaría la creación de empleo y especialización de profesionales en la materia.

18. Las sanciones fijadas por la Ley son excesivas

El tabulador de sanciones en el caso mexicano (arts. 64 a 66 LPDP), es más elevado que el español, aunque con la significativa mención de la Ley en atender a la “capacidad económica del responsable”, lo que habrá de determinarse por la autoridad competente. Por otro lado, se encuentran tipificados en la propia Ley de protección de datos, los delitos en materia de tratamiento indebido de datos personales. Ambas situaciones, constituyen por si solas un incentivo para el cumplimiento de la Ley. Sin embargo, y por ser una legislación nueva, mientras

no se comience a llevar a cabo las multas y tipificaciones de delitos, la normativa no solo no se cumplirá, sino que se vulnerará deliberadamente.

19. Es acertada la tipificación de los delitos especiales

Es interesante y acertada la tipificación de delitos en el capítulo XI de la Ley Federal de protección de datos personales en posesión de los particulares, sobre delitos en materia del tratamiento indebido de datos personales, que regula los actos constitutivos de delitos especiales en esta área. Esto es una novedad legislativa, por no encontrarse tipificados dentro de la propia Ley de la materia en otros países como España, Argentina, Costa Rica o Perú.

20. Necesidad del Habeas Data como una garantía constitucional adicional.

El habeas data es una garantía constitucional existente en países latinoamericanos, cuya diferencia principal radica en ser un Recurso que se promueve ante un órgano judicial, y no de un procedimiento de naturaleza administrativa, como es el caso de los países europeos. Esto responde a necesidades históricas propias de los sistemas de gobierno dictatoriales que hubo en América Latina.

Estamos de acuerdo con la garantía que proporciona un órgano administrativo especializado en la materia. Sin embargo, a la par de ello, es conveniente, principalmente para la fortificación del derecho fundamental, que se prevea el recurso de Habeas Data en México, para situaciones de máxima seguridad como por ejemplo los que tienen que ver con los datos sensibles, seguridad y defensa de grandes colectivos, así como los que se refieren a evidentes intereses nacionales.

21. Necesidad de configuración constitucional interpretativa del Poder Judicial Federal

Finalmente, se reitera la existe de la necesidad de que el Instituto emprenda una trascendental labor de divulgación, mediante la cual la ciudadanía conozca la existencia de este nuevo derecho y de los mecanismos para hacerlo

valer. Así, el IFAI emitirá resoluciones, que eventualmente serán recurridas ante el Poder Judicial Federal y este dictará Sentencias que habrán de aclarar y configurar cada día este nuevo derecho.

V. Conclusioni

Il diritto alla protezione dei dati personali è un prodotto tipico dell'epoca attuale, corollario dall'evoluzione delle nuove tecnologie. Il presente studio si concentra sull'analisi delle principali caratteristiche e differenze di tale diritto che si sono dovute adottare nel caso spagnolo e messicano. In questo senso, i risultati hanno evidenziato i principali elementi di carattere storico che hanno determinato la configurazione di tale diritto fino ai nostri giorni.

La presente ricerca è stata strutturata in funzione di quattro ambiti, ognuno importante per un'adeguata comprensione del tema, a partire dai caratteri generali dell'origine del diritto alla protezione dei dati personali, sino alle sue prime introduzioni costituzionali. Si è inoltre trattato il tema attraverso lo studio del caso spagnolo in quanto principale referente in Messico, concludendo con la situazione attuale dello Stato Messicano e della sua recente legislazione in questo ambito. Attraverso questa traiettoria di ricerca si è giunti alle seguenti riflessioni:

1 Autonomia del diritto fondamentale alla protezione dei dati personali per quanto riguarda la sua definizione, ma di difficile emancipazione pratica nel suo atto di esercizio in relazione alla privacy.

Concordiamo sul fatto che si tratta di un diritto che ha autonomia propria, per quanto riguarda la sua definizione e delimitazione giurisprudenziale, sebbene risulta alla pratica ancora strettamente legato al diritto della privacy. Ciò si deve al fatto che, nell'atto di esercizio del diritto alla protezione dei dati personali, si tutela fundamentalmente anche il diritto alla privacy, in alcuna delle sue forme.

Ciò nonostante, il diritto alla protezione dei dati si manifesta come un diritto indipendente che risponde a diverse necessità – rispetto del diritto alla privacy -, dall'inadeguata gestione manuale dei dati personali da parte di chi è in possesso dell'informazione, fino a pericoli reali dovuti a vari metodi di automatizzazione di procedimenti e fuga di informazioni personali individuali. La STC 292/2000 ha dovuto differenziare la riservatezza dal diritto alla protezione dati per quanto concerne la sua funzione, oggetto e contenuto.

2 Esiste un'utile delimitazione giurisprudenziale del Tribunale Costituzionale spagnolo del diritto alla protezione dei dati personali in merito alla funzione, l'oggetto e il contenuto, la quale contribuisce a differenziarlo dal diritto alla riservatezza.

Per quanto riguarda la delimitazione del diritto alla protezione dati in merito alla riservatezza, concordiamo con quella fornita dal Tribunale Costituzionale spagnolo nella Sentenza 292/2000. Per quanto concerne la sua “*funzione*”, sottolinea che il *diritto alla riservatezza* protegge l'individuo da qualsiasi invasione nella sua vita personale e familiare, cioè, il potere di proteggere la sua vita privata da una pubblicità indesiderata. Dall'altro lato, il *diritto alla protezione dati* mira a garantire alla persona un potere di controllo dei propri dati personali, il suo uso e finalità, con l'obiettivo di impedire il suo traffico illecito e nocivo alla dignità e al diritto dell'interessato. Tale diritto garantisce il potere individuale di disporre dei dati personali.

Per quanto riguarda l'“*oggetto*” di entrambi i diritti, la singolarità del diritto alla tutela dei dati risulta un oggetto più ampio in confronto al diritto alla riservatezza. Il diritto alla *protezione dati* estende la garanzia costituzionale a quei dati che siano rilevanti o abbiano un effetto nell'esercizio di qualsiasi diritto della persona, a prescindere che si tratti o no di diritti costituzionali o siano o no relativi all'onore, all'ideologia, alla riservatezza personale e familiare, e a qualsiasi altro bene protetto costituzionalmente. L'oggetto della protezione si estende altresì a quei dati personali pubblici che non esulano dal potere di disposizione della persona interessata come stabilito dal diritto alla protezione dei dati. Anche per questo motivo, il fatto che i dati non siano di carattere personale non comporta che siano protetti solo quelli relativi alla vita privata o intima della persona. I dati sotto protezione giuridica sono infatti tutti quelli che identificano o permettono l'identificazione della persona, e che possano servire alla configurazione di qualche profilo della personalità.

In quanto al diverso “*contenuto*” di entrambi i diritti, la Sentenza sancisce che il diritto alla riservatezza personale o familiare conferisce alla persona il potere giuridico di imporre a terzi l'obbligo di astenersi da qualsiasi

intromissione nella sfera intima della persona, e il divieto di fare uso di ciò che si è venuto a conoscenza. Mentre il diritto alla protezione dei dati attribuisce al titolare una sfera di facoltà e poteri giuridici il cui esercizio impone doveri giuridici a terzi, garantisce tuttavia un potere di controllo e disposizione da parte dell'individuo dei propri dati personali. Ciò è possibile e attuabile solo attraverso l'imposizione a terzi i su menzionati diritti con il fine di rispettare i diritti del titolare che sono: il diritto a che sia previamente richiesti l'autorizzazione alla raccolta e all'uso dei dati personali, il diritto a sapere ed essere informato in merito alle finalità e all'uso di tali dati, e il diritto ad accedere, rettificare e cancellare gli stessi. In definitiva, il potere di disposizione dei dati personali.

3. Necessità di standardizzazione della normativa a livello internazionale affinché si rifletta in ambito nazionale.

Al giorno d'oggi, per via dell'istantaneità e ubiquità della società nell'era della globalizzazione, il comportamento degli individui ha teso a omogeneizzarsi a livello culturale, così come la soluzione alle necessità e l'espansione dei problemi che le nuove tecnologie hanno comportato. Per esempio il *cloud computing*, una recente maniera di archiviazione dati, comporta nuovi scenari nel trattamento, trasmissione e gestione delle informazioni, i quali hanno reso difficoltoso il compimento dell'attuale normativa di ogni paese. Di conseguenza, la regolamentazione legale del tema si manifesta come una necessità dalla soluzione ancora irrisolta, così come l'impulso di una legislazione internazionale standardizzata che permetta l'aggregazione di tutti i migliori strumenti attualmente in circolazione.

4. Il diritto alla protezione dei dati personali può entrare in conflitto con altri diritti fondamentali, creando un problema che si dovrà risolvere attraverso una ponderazione adeguata di ogni singolo caso.

L'evoluzione legislativa che ha portato alla configurazione di questo diritto non è stata rapida, né spontanea, ma si è sviluppata lentamente. Ha risposto, infatti, alle necessità dell'individuo di avere un controllo delle proprie informazioni personali, diventando un ulteriore mezzo di tutela di altri diritti

fondamentali, come la dignità, la privacy, la propria immagine, l'onore, la vita, l'informazione, ecc.

In questo senso, il diritto alla protezione dei dati personali può entrare in conflitto con il diritto all'informazione, sfociando in una situazione che può essere risolta attraverso un'adeguata ponderazione dei diritti. Tuttavia, nell'attività degli organi dell'Amministrazione Pubblica, si dovrà dare la precedenza alla massima trasparenza per via dell'origine delle sue entrate derivanti dalle imposte sui cittadini, ad eccezione delle restrizioni richieste dalla legge. È inoltre da segnalare che esisteranno ulteriori casi in cui sarà necessaria una corretta ponderazione di entrambi i diritti in merito al caso specifico, tenendo in considerazione l'interesse pubblico, e il grado e la misura in cui viene coinvolto il titolare dell'informazione. In Messico, come disposto dalla Risoluzione 932/2005 emessa l'11 Giugno dall' IFAI (in allegato), da diversi anni vi è stata un'evoluzione nella pubblicazione delle remunerazioni degli impiegati statali poiché provenienti dal contributo dei cittadini, e sarebbe un passo indietro che dall'introduzione di questo diritto in Messico si giunga a sostenere che detta informazione risulta un dato personale di carattere patrimoniale e di conseguenza non suscettibile di rivelazione pubblica.

5. In confronto alla Spagna, il Messico presenta un ritardo di quasi venti anni, che lo rende vulnerabile nell'attuale era della globalizzazione e cambio strutturale della società.

Attualmente la società attraversa un cambio strutturale dovuto alla globalizzazione e alle nuove tecnologie, che mette in relazione gli individui in funzione di diversi ruoli. Per questo motivo, l'informazione risultante da queste interazioni deve preservare diritti della persona come la privacy e la protezione dei dati personali.

In questo senso, come si deduce dall'analisi dei sistemi giuridici messicani e spagnoli in materia di protezione dati, non si è verificato un costante confronto parallelo, poiché l'avvento del diritto non si è manifestato nella stessa linea temporale. In confronto alla Spagna, il Messico presenta un ritardo di 18 anni dalla pubblicazione della prima normativa spagnola in materia di protezione

dati del 1992 (LORTAD) – la successiva e attualmente vigente è la LOPD del 1999 – alla Legge messicana del 2010. Questa situazione rende il paese vulnerabile poiché lo stato messicano sta attraversando il processo d'implementazione e adattamento della normativa, così come di sensibilizzazione da parte della popolazione. Tale vulnerabilità si manifesta per via dell'assenza di un'adeguata delimitazione giudiziaria e giurisprudenziale del diritto, che non sorprende data la sua recente introduzione nell'ordinamento giuridico.

6. Esiste una prima apparizione del diritto alla protezione dei dati personali in Messico, che si è rivelato poco efficace e limitato nel suo esercizio in ella sua garanzia nel 2002.

Il diritto alla protezione dei dati personali in Messico fa la sua prima apparizione nel 2002 nella Legge Federale sulla Trasparenza e l'Accesso all'informazione Pubblica Governativa; e successivamente con le riforme costituzionali del 2009 degli articoli 16 e 73 della Costituzione. L'evoluzione legislativa si conclude recentemente con la pubblicazione della Legge Federale per la Protezione dei Dati Personali in Possesso dei Soggetti privati (2010), e il suo Regolamento (2011). Questa prima apparizione si è rivelata poco efficace, poiché a quel tempo nella Legge sulla Trasparenza si faceva riferimento solo ai dati personali in possesso dell'amministrazione pubblica e non a quelli in possesso dei soggetti privati, come avviene oggi.

Si noti inoltre come questa succinta regolazione del diritto alla protezione dati compare nel 2002 in Messico in contemporanea con la Legge sulla Trasparenza. Di conseguenza, e data la storia del paese in tema di corruzione, lo sforzo è stato condotto ai fini di detta Legge, cioè alla trasparenza e all'accesso all'informazione pubblica: senza che il diritto alla tutela dei dati personali fosse sviluppato adeguatamente. Oggigiorno, il diritto alla trasparenza si trova in uno stato di maturità, e le necessità della società attuale richiedono la consolidazione del diritto alla tutela dei dati personali, al fine di avere il potere di disporre delle proprie informazioni.

7. La legge spagnola di protezione dati è fonte ispiratrice dell'attuale norma messicana.

Corollario dei vincoli storici e della cooperazione con la Spagna, dall'analisi della Legge messicana si deduce la profonda influenza dell'esperienza spagnola, e i principali temi di discussione tra gli esperti del settore, derivanti dalla realtà tecnologica del momento come ad esempio il *cloud computing* nell'articolo 52 RLOPD, una nuova forma di archiviazione di informazioni dalla difficile regolazione per via della mancanza di una legislazione internazionale standardizzata. La stessa osservazione è valida in merito alla chiarificazione del diritto di opposizione nella Legge (articoli 8 e 27 LPDP), la cui omissione nella Legge spagnola ha dato luogo a qualche critica (articoli 34-36 RLOPD), che risulta invece una chiara rettificazione nella legge messicana.

Il diritto spagnolo in materia si è evoluto grazie alla sua pratica in altre latitudini del continente europeo. Tale processo si è nutrito non solo dell'introduzione delle diverse normative in Europa, ma anche dell'attività dell'*Agencia Española de Protección de Datos* e dei suoi corrispettivi nelle comunità autonome, insieme alla dottrina emessa dal Tribunale Costituzionale. Tale esperienza ha fatto breccia in America Latina e contribuito alla legislazione esistente in materia.

8. Necessità di diffondere il diritto alla tutela dei dati personali nella popolazione in maniera chiara, seria e impegnata da parte delle autorità.

Oggi in Messico viene riconosciuta l'importanza del diritto fondamentale per la protezione dei dati personali, e si può contare, seppur tardivamente, su di una Legge specializzata e dal suo Regolamento. Di conseguenza, è più che mai opportuna l'attuazione da parte dei titolari del diritto di farlo rispettare, altrimenti l'esercizio di tale diritto brillerà della sua assenza, fin quando gli individui non siano a conoscenza dei diritti e delle azioni di cui possono avvalersi.

9. La configurazione messicana dell'avviso di privacy ordinato dalla stessa legge, è una novità.

Una delle differenze dell'ordinamento messicano rispetto a quello spagnolo è che l'avviso di privacy è regolato dalla Legge e dal suo Regolamento.

Da un lato, la Spagna lo regola unicamente attraverso il Regolamento. Il Ministero dell'Economia messicana, invece, con il contributo dell'Istituto, è responsabile dell'emissione delle linee corrispondenti relative al contenuto e alla portata dell'avviso di privacy. Di conseguenza, nel giugno del 2011 è stata pubblicata la Guida pratica per la produzione dell'avviso di privacy (ma non le linee), in cui si stabiliscono le responsabilità del trattamento dei dati personali in merito all'elaborazione, la progettazione e la diffusione dell'avviso di privacy. Tale guida completa e semplifica ampiamente le richieste della Legge in merito a detto avviso.

10. La complessità del formato della informativa sulla privacy indicata dalla legge rende difficile l'adattamento della normativa.

La Guida in merito all'avviso di privacy emessa dal Ministero dell'Economia, specifica che l'avviso, completo o semplificato, varierà di lunghezza in funzione di diversi fattori come: lo spazio per aggregare l'avviso, il mezzo con cui si raccoglie l'informazione, il tipo di dati raccolti e se è previsto o no un trasferimento. In quest'ultimo caso, l'autorizzazione al trasferimento internazionale è data per difetto, salvo che il titolare si opponga alla stessa segnando la casella corrispondente. Nel caso l'avviso non contempli uno spazio sufficiente, il titolare dovrà ricercare l'avviso completo.

Di conseguenza non c'è da stupirsi che la questione dell'avviso di privacy, nonostante gli sforzi per renderlo conforme a diritto, risulti confuso. Questo fa sì, inoltre, che il rinvio al documento completo contenga un certo livello di poca chiarezza nella manifestazione della volontà, diventando fonte di diffidenza per il cittadino. L'avviso completo è assimilabile a un contratto breve e con un certo livello di difficoltà, il che è reso ancor più complesso nel caso di una normativa di nuova implementazione, la quale dovrebbe essere invece uno strumento semplice e totalmente avverso a una situazione di poca praticità a fini di diffusione e sensibilizzazione.

11. Si avverte la necessità di omogeneizzare i principi del trattamento nella normativa messicana di protezione dei dati personali del settore pubblico e privato.

I principi che dovranno osservare i responsabili assecondano l'obiettivo della necessità del momento e sono conformi alle richieste internazionali. Ciò nonostante, poiché si fa riferimento a una regolazione che distingue tra i dati in possesso del settore pubblico e del privato, si consiglia un'adeguata unificazione per rendere più chiara la normativa di questo nuovo diritto per l'utente. Nel caso del settore pubblico, i principi vengono contemplati nelle Linee Guida e non in un Regolamento come nel caso del settore privato.

La lista dei principi nei due settori non sono esattamente identici per quanto riguarda la loro denominazione e contenuto. Nella regolazione del settore pubblico, a differenza di quello privato ad esempio, non vengono chiaramente contemplati principi come finalità, lealtà, proporzionalità e responsabilità; che si apprezzano tuttavia nell'insieme della definizione delle qualità del principio come: esatto (lealtà), adeguato (responsabilità), pertinente (finalità e responsabilità) e non eccessivo (proporzionalità, lealtà e finalità). Dal canto suo, il principio della Sicurezza che si trova in questa sezione, la cui nomenclatura nel caso dei soggetti privati è "Responsabilità", non specifica in pieno l'aspetto del dovere del segreto.

Tra i principi del settore privato inoltre, notiamo come quello della legittimità (articolo 7 LPDP e articolo 10 RLPDP) ad esempio, deve essere osservato durante la raccolta e il trattamento dei dati. In questo caso, il Regolamento della Legge adduce che tale trattamento dovrà essere effettuato in conformità con la legislazione messicana in materia e con il diritto internazionale. Quest'ultima menzione è degna di nota non solo per gli strumenti internazionali regionali esistenti in Europa (che non sono vincolanti, ma piuttosto orientativi), ma anche per via dell'attuale tendenza verso la standardizzazione della normativa del diritto alla protezione dei dati personali. Di conseguenza non ci si stupirà che in futuro possano essere introdotti strumenti regolatori in materia.

12. Il tacito assenso è un'innovazione.

Per quanto riguarda il principio dell'assenso, si stabiliscono due tipi: esplicito e tacito. Quest'ultimo, a differenza di altri paesi, è una novità messicana, e consiste in ciò che si autorizza quando, una volta che ci si avvale dell'avviso di

privacy, il titolare non manifesta dissenso. Il tacito assenso sarà valido come regola generale, a meno che la Legge richieda l'assenso esplicito (articoli 13 e 14 RLPDP). Per via della recente innovazione di questa tipologia, dunque, il regolamento non è chiaro nel meccanismo che si dovrà adottare nello stesso avviso di privacy, affinché il titolare possa manifestare il suo dissenso al trattamento.

13. Armonizzazione del trattamento a livello internazionale.

La legge messicana menziona gli schemi di autoregolazione, tradotti in codici deontologici o sigilli di confidenza. La visione previa è significativa al fine di standardizzare e armonizzare i trattamenti dei dati, oltre a facilitare lo sforzo dell'Istituto, mediante la collaborazione nella diffusione del diritto e nel compimento della Legge. Ciò nonostante, poiché il Messico sta attraversando un processo d'implementazione di questa nuova normativa, sarebbe opportuno che l'Istituto chiarisca dettagliatamente quali sono tali schemi.

14. Necessità di un certificato che attesti l'effettivo compimento della normativa relativa alla protezione dei dati personali in Messico.

Allo stesso modo, affinché esistano certificazioni internazionali in questo ambito, risulta fondamentale la creazione di un meccanismo simile valido a livello nazionale, regolato dall'Istituto e la cui licenza sia autorizzata a professionisti tecnico-specializzati in materia. Ciò si rivelerà un passo essenziale verso l'urgente omogeneizzazione dei processi nella protezione dei dati. In questo modo sarà promosso l'interesse della comunità giuridica in questo settore, comportando progressi significativi nel compimento della LPDP, oltre a incoraggiare la cooperazione e la partecipazione internazionale in questo campo.

15. Necessità di un Registro Schedari.

A differenza di quella spagnola, la Legge messicana rappresentata dall'Autorità regolatrice non contempla un Registro Schedari. Ciò può rappresentare un pericolo per l'individuo da parte del Responsabile o incaricato. Se chi compila il formulario non conosce bene la legge né i dati che possono essere trattati – cosa non rara durante la fase d'implementazione di una nuova

normativa – esiste il pericolo di creare schedari e trattare informazioni in eccesso, poiché non si è correttamente informati. L'iscrizione di schedari è una misura che in questo caso potrebbe prevenire l'archiviazione di dati personali in un database non chiaro, che possa posteriormente risultare illegale.

16. Necessità di livelli di sicurezza regolati.

La normativa messicana non prevede l'implementazione di differenti gradi di sicurezza in base al tipo di dati personali da trattare. Le misure previste dal Regolamento possono dar luogo a dubbi per i quali sarebbe opportuno uno strumento speciale che regoli diversi tipi di sicurezza a cui il Responsabile o l'incaricato debba attenersi.

17. Necessità della responsabilità dello Specialista protezione dati.

La presenza di una persona responsabile al compimento della normativa per la protezione dei dati in ogni impresa o istituzione risulta opportuna per un'adeguata implementazione della Legge. Tale pratica sarebbe inoltre un incentivo per la creazione di occupazione e specializzazione professionale in materia.

18. Le sanzioni previste dalla Legge sono eccessive.

Nel caso messicano il tabulatore delle sanzioni (articoli 64-66 LPDP) è più elevato che quello spagnolo, sebbene sia significativa la menzione della Legge alla considerazione della "capacità economica del responsabile", da determinarsi da parte dell'autorità competente. D'altro lato, la stessa Legge per la protezione dei dati riconosce i crimini in materia di trattamento indebito di dati personali. In entrambi i casi, costituiscono di per sé un incentivo per il compimento della Legge. Ciò nonostante, poiché si tratta di una nuova legislazione, finché non si comincerà a comminare multe e specificare la tipizzazione dei crimini, non solo la normativa non si compirà, ma risulterà deliberatamente vulnerabile.

19. La tipizzazione dei crimini speciali è appropriata.

La tipizzazione dei crimini nel capitolo XI della Legge Federale sulla protezione dei dati personali in possesso dei soggetti privati risulta interessante e appropriata, in merito ai crimini in materia del trattamento indebito dei dati personali, che regola gli atti costitutivi dei crimini speciali in quest'area. Si tratta, questa, di una novità legislativa, poiché non si trova tipificata all'interno della stessa Legge in materia in altri paesi come Spagna, Argentina, Costa Rica e Perù.

20. Necessità dell'*Habeas Data* come garanzia costituzionale aggiuntiva.

L'*habeas data* è una garanzia costituzionale esistente in paesi latinoamericani, la cui differenza principale si fonda sul fatto di essere una risorsa a cui si ricorre di fronte ad un organo giudiziale, e non di un procedimento di natura amministrativa, come nel caso dei paesi europei. Ciò risponde a necessità storiche proprie dei sistemi di governo dittatoriali del passato latinoamericano.

Concordiamo con la garanzia data da un organo amministrativo specializzato in materia. Ciò nonostante, e di pari importanza, è opportuno che sia previsto il ricorso all'*Habeas Data* in Messico, principalmente al fine di fortificare il diritto fondamentale in situazioni di massima sicurezza, ad esempio quelli che coinvolgono i dati sensibili, la sicurezza e la difesa di grandi collettivi, e quelli riguardanti evidenti interessi nazionali.

21. Necessità di una configurazione costituzionale interpretativa del Potere Giudiziale Federale.

Ribadiamo infine la necessità da parte dell'Istituto di intraprendere un'opera trascendentale di divulgazione, attraverso la quale i cittadini vengano a conoscenza di questo nuovo diritto e dei meccanismi con cui avvalersene. L'IFAI emetterà delle risoluzioni a cui si farà eventualmente appello di fronte al Potere Giudiziale Federale, il quale emetterà delle Sentenze che dovranno quotidianamente chiarificare e configurare questo nuovo diritto.

Bibliografía

1. Monografías

- Acciai, R. (2004). *Il diritto alla protezione dei dati personali*. Santarcangelo di Romagna, Rimini: Maggioli.
- Aced Felez, E. (2000). Transacciones electrónicas en Internet. En A. d. Datos, *Jornadas sobre protección de la privacidad. Telecomunicaciones e Internet. Pamplona, 22 y 23 de junio de 2000*. (pág. 99 a 120). Pamplona: Universidad Pública de Navarra.
- Agencia de Protección de Datos de la Comunidad de Madrid. (2004). *Repertorio de legislación y jurisprudencia sobre protección de datos*. Madrid: APDCM- Thomson Civitas.
- Agencia de Protección de Datos de la Comunidad de Madrid. (2008). *Protección de Datos Personales para Corporaciones*. Madrid: Thomson Civitas.
- Agencia de Protección de Datos de la Comunidad de Madrid. (2009). *Seguridad y protección de datos personales*. Madrid: Thomson Civitas.
- Agencia Española de Protección de Datos. (2011). Modulo 6. El derecho a la protección de datos en iberoamerica. En D. Doneda, & R. García Gonzalo, Curso: El derecho a la protección de datos personales, 3ª edición. Madrid, España: AEPD, AECID y Fundación CEDDET.
- Amoroso Fernández, Y. (marzo de 1991). La informática como objeto de Derecho. Algunas consideraciones acerca de la protección jurídica en Cuba de los datos automatizados. *Revista cubana de Derecho, Vol. VII*(No. 1), 40-52.
- Arenas Ramiro, M. (2006). *El derecho fundamental a la protección de datos personales en Europa*. Valencia: Tirant lo blanch.
- Balaguer Callejón, M. L. (1992). *El derecho fundamental al honor*. Madrid: Tecnos.

- Ballesteros Moffa, L. A. (2005). *La privacidad electrónica*. Valencia: Tirant lo blanch.
- Bartolome Cenzano, J. C. (2003). *Derechos fundamentales y libertades públicas*. Madrid: Tirant lo blanch.
- Blanco Restrepo, J. H., & Maya Mejía, J. M. (2005). *Fundamentos de Salud Pública. Tomo I. Salud Pública* (2ª. ed.). Medellín, Colombia: Corporación para Investigaciones Biológicas.
- Bobbio, N. (1991). *El tiempo de los derechos*. Madrid: Sistema.
- Bobbio, N. (1996). *El futuro de la democracia*. (J. F. Santillán, Trad.) México: Fondo de Cultura Económica.
- Caballero Gea, J.-A. (2007). *Derecho al honor, a la intimidad personal y familiar y a la propia imagen. Derecho de rectificación, calumnia e injuria*. Madrid: Dykinson.
- Caballero Juárez, J. A., Díaz, V., & Villanueva, E. (2006). *Derecho de acceso a la información en el Poder Judicial*. México: H. Cámara de Diputados LIX LEGislatura, Libertad de Información México A.C., Fundación Konrad Adenauer y Miguel Angel Porrúa.
- Calderon Arozqueta, J. L., & Salgado Garza, E. (2000). El estudio de la seguridad nacional y la inteligencia en México. *Revista de Administración Pública*(Num. 101), 97-105.
- Callejo Carrión, S. (2006). *El derecho al honor. El honor como objeto del proceso civil de amparo especial*. Madrid: Grupo Difusión.
- Campuzano Tomé, H. (2000). *Vida privado y datos personales*. Madrid: Tecnos.
- Carpizo Mc-Gregor, J. (mayo-junio de 1993). Los derechos de la tercera generación: paz y desarrollo. *Cuadernos Americanos, Vol. 3*(Novena Epoca, Año VII, No. 39).

- Carpizo Mc-Gregor, J., & Gómez-Robledo Verduzco, A. (enero-abril de 2000). Los tratados internacionales, el derecho a la información y el respeto a la vida privada. *Boletín mexicano de Derecho Comparado*(Año XXXIII, No. 97), 9-63.
- Carranza Torres, L. R. (2001). *Habeas data. La protección jurídica de los datos personales*. Argentina: Alveroni.
- Carrillo Salcedo, J. A. (2003). *El convenio europeo de derechos humanos*. Madrid: Tecnos.
- Cesario, R. (2001). *Hábeas data. Ley 25.326*. Buenos Aires: Editorial Universidad.
- Cifuentes, S. (2007). El derecho a la vida privada. Tutela a la intimidad. Buenos Aires: La Ley.
- Comella, C. (2006). Privacy e nuove tecnologie. En P. Cendon, *Libera circolazione e protezione dei dati personali*. Trattati, Tomo II (págs. 1241-1259). Milano: Giuffrè.
- Conde Ortiz, C. (2005). *La protección de datos personales: un derecho autónomo con base en los conceptos de intimidad y privacidad*. Madrid: Dykinson.
- Contreras Peláez, F. J. (1994). *Derechos sociales: teoría e ideología*. Madrid: Tecnos.
- Corripio Gil-Delgado, M. d. (2000). *Regulación jurídica de los tratamientos de datos personales realizados por el sector privado en Internet*. Madrid: Agencia de Protección de Datos.
- Corripio Gil-Delgado, M. d., & Marroig Pol, L. (2001). *El tratamiento de los datos de carácter personal y la protección de la intimidad en el sector de las telecomunicaciones*. Madrid: Agencia de Protección de Datos.
- Cortés Bechiarelli, E. (1998). *El secreto profesional del abogado y del procurador y su proyección penal*. Barcelona: Marcial Pons.

- Crevillén Sánchez, C. (1994). *Derechos de la personalidad. Honor, intimidad personal y familiar y propia imagen en la jurisprudencia*. Madrid: Actualidad.
- Curzio, L. (2007). *La seguridad nacional en México y la relación con Estados Unidos*. México: Universidad Nacional Autónoma de México y Centro de Investigaciones sobre América del Norte.
- Dávora Fernández de Marcos, I. (2011). *Hacia la estandarización de la protección de datos personales*. Madrid: La Ley.
- Dávora Rodríguez, M. A. (2004). *Anuario de derecho de las tecnologías de la información y las telecomunicaciones (TIC)*. España: Dávora & Dávora.
- Dávora Rodríguez, M. A. (2005). *Anuario de derecho de las tecnologías de la información y las telecomunicaciones (TIC)*. España: Dávora & Dávora.
- De Bartolomé Cenzano, J. C. (2002). *El orden público como límite al ejercicio de los derechos y libertades*. Madrid: CEPC.
- De Koninck, T. (2006). *De la dignidad humana*. (M. V. Grau, Trad.) Madrid: Dykinson.
- Del Castillo Vázquez, I.-C. (2007). *Protección de datos: cuestiones constitucionales y administrativas. El derecho a saber y la obligación de callar*. Madrid: Thomson-Civitas.
- Del Peso Navarro, E, & Ramos González, M.A. (2002). *La seguridad de los datos de carácter personal* (2ª ed.). Madrid: Díaz de Santos.
- Del Peso Navarro, E. (2003). *Servicios de la sociedad de la información* (2 ed.). Madrid: Díaz de Santos.
- Delgado Triana, Y. (2008). *Protección en el ordenamiento jurídico cubano de los derechos inherentes a la personalidad en la esfera moral*. Cuba: Editorial Universitaria.

- Desantes Guanter, J. M. (1974). *La información como derecho*. Madrid: Editora Nacional.
- Desantes Guanter, J. M. (1976). *La función de informar*. Pamplona: Universidad de Navarra.
- Díaz-Arias, J. M. (2008). *Guía práctica sobre normativa de protección de datos y publicidad comercial*. Barcelona: Deusto.
- Domínguez González, L. A. (2010). *Transparencia de la información pública y protección de datos personales: un balanceo necesario*. Madrid: Servicio de Publicaciones de la Facultad de Derecho de la Universidad Complutense de Madrid.
- Donaires Sánchez, P. (2001/2002). Los derechos humanos. *Revista Telemática de Filosofía del Derecho*(No. 5), 193-199.
- Ekmekdjian, M. A. (1996). *Habeas data. El derecho a la intimidad frente a la revolución informática*. Buenos Aires: Depalma.
- Esquinas Valverde, P. (2010). *Protección de datos personales en la Policía Europea*. Valencia: Universidad de Granada & Tirant lo blanch.
- Fernández Delpech, H. (2001). *Internet: su problemática jurídica*. Buenos Aires: Abeledo-Perrot.
- Fioriglio, G. (2008). *Il diritto a la privacy. Nuove frontiere nell'era di internet*. Bologna: Bologna University Press.
- Flores Dapkevicius, R. (2004). *Amparo, hábeas corpus y hábeas data*. (J. C. S.R.L., Ed.) Montevideo-Buenos Aires, Uruguay-República Argentina: B de F Ltda.
- Frosini, V. (1981). *Il Diritto nella società tecnologica*. Milano: Giuffrè editore.
- Frosini, V. (1982). *Cibernética, Derecho y Sociedad*. Madrid: Tecnos.
- García García, C. (2003). *El derecho a la intimidad y dignidad en la doctrina del Tribunal Constitucional*. España: Universidad de Murcia.

- García Jiménez, M. E. (1998). *El convenio europeo de derechos humanos en el umbral del siglo XXI*. Valencia: Tirant lo blanch y Universitat de València.
- García P., G. (2009). Derecho de acceso a la información en Chile: nueva regulación e implicancias para el sector de la defensa nacional. *Estudios Constitucionales. Revista semestral del Centro de Estudios Constitucionales de Chile*.(Año 7, No. 1), 137-175.
- García Roca, J., & Santolaya, P. (2005). *La Europa de los derechos. El convenio europeo de derechos humanos*. Madrid: Centro de Estudios Políticos y Constitucionales.
- García-Berrio Hernández, T. (2003). *Informática y libertades: la protección de datos personales y su regulación en Francia y España*. Murcia: Servicio de Publicaciones de la Universidad de Murcia.
- Garriga Domínguez, A. (2004). *Tratamiento de datos personales y derechos fundamentales*. Madrid: Dykinson.
- Gómez Gómez, A. (2006). *Cincuentenario de la declaración universal de derechos humanos*. Colombia: Red Reflexión Política.
- Gómez Navajas, J. (2005). *La protección de los datos personales. Un análisis desde la perspectiva del Derecho Penal*. Navarra: Thomson-Aranzadi.
- Gómez-Robledo Verduzco, A., & Ornelas Núñez, L. (2006). *Protección de datos personales en México: el caso del Poder Ejecutivo Federal*. México: UNAM.
- González Pascual, M. (septiembre/diciembre de 2009). El Tribunal Constitucional Federal almenán ante la compatibilidad con los derechos fundamentales de la normativa nacional de origen europeo de prevención de delitos. *Revista de Derecho Comunitario Europeo*(No. 34, año 13), 945-966.

- González Pérez, L. R. (Julio-Diciembre de 2007). Libertad de expresión, seguridad pública y poderes facticos. *Derecho Comparado de la Información* (Num. 10).
- Goñi Sein, J. L. (2007). La videovigilancia empresarial y la protección de datos personales. Pamplona: Thomson-Civitas y Agencia de Protección de Datos de la Comunidad de Madrid.
- Gozaíni, O. A. (2002). *Derecho Procesal Constitucional. Hábeas Data. Protección de datos personales. Ley 25.326 y reglamentación (decreto 1558/2001)*. Buenos Aires: Rubinzal-Culzoni.
- Granados Pérez, C. (1999). Jursiprudencia del Tribunal Supremo sobre el derecho al honor, a la intimidad y a la propia imagen. En E. Torres-Dulce Lifante, *Derecho al honor, a la intimidad y a la propia imagen* (págs. 130-244). Madrid: Consejo General del Poder Judicial.
- Guerrero Picó, M. d. (2006). *El impacto del Internet en el derecho fundamental a la protección de datos de carácter personal*. Navarra: APDCM, Aranzadi, Thomson-Civitas.
- Guichot, E. (2009). *Publicidad y privacidad de la información administrativa*. España: Thomson-Civitas, Aranzadi y APDCM.
- INTECO. (2009). Guía legal sobre ciberbullying y grooming. Instituto Nacional de Tecnologías de la Comunicación, Observatorio de la Seguridad de la Información mediante el área jurídica de la seguridad y las TIC. Madrid: INTECO.
- Kagan, S. (2010). Obscenity on the Internet: Nationalizing the Standard to Protect Individual Rights. *Hastings constitutional law quarterly*, Vol. 38(Num. 1), 233-257.
- Landa, C. (julio-diciembre de 2002). Dignidad de la persona humana. *Cuestiones Constitucionales. Revista Mexicana de Derecho Constitucional*(No. 7), 109-138.

- Lasagabaster Herrarte, I. (2004). *Convenio europeo de derechos humanos*. Madrid: Thomson-Civitas.
- Lesmes Serrano, C., Buisán García, N., Fernández García, J. A., Guerrero Zaplana, J., & Sanz Calvo, L. (2008). *La Ley de Protección de Datos. Análisis y comentario de su jurisprudencia*. (1a. ed.). España: Lex Nova.
- López Chavarría, J. L. (enero-junio de 2005). Análisis de la reforma constitucional y de la iniciativa de ley sobre seguridad nacional. *Cuestiones Constitucionales. Revista mexicana de Derecho Constitucional*(Num. 12), 293-315.
- Lyon, E. (2009). "A Picture is Worth a Thousand Words": the Effect of Spectators' Display of Victim Photographs During a Criminal Jury trial on a Criminal Defendant's Fair Trial Rights. *Hastings constitutional law quarterly*, Vol. 36(Num. 3), 517-544.
- Magallón, J. M. (Julio-Diciembre de 1965). El orden público como sistema de solución al conflicto de leyes. *Revista de la Facultad de Derecho de México*(Num. 59), 661-682.
- Mansilla y Mejía, M. E. (Enero-Febrero de 2003). Naturaleza jurídica del orden público en el Derecho Internacional Privado. *Anales de Jurisprudencia*(Num. 261), 333-351.
- Marafioti, L. (2010). Derecho comparado: medidas de prevención, represión y control del dopaje en el Derecho italiano deportivo y penal. Referencia a los riesgos para la intimidad. En A. Doval Pais, & N. Sánchez-Moraleda, *Dopaje, intimidad y datos personales. Especial referencia a los aspectos penales y político-criminales* (págs. 75-86). España: Iustel.
- Marcoccia, E. (2006). La tutela dei minori. En P. Cendon, *Libera circolazione e protezione dei dati personali*. Trattati, Tomo I. (págs. 331-528). Milano: Giuffrè.
- Martí Capitanachi, L. d. (2007). *Democracia y derecho a la información*. México: Porrúa.

- Martin Morales, R. (1995). *El régimen constitucional del secreto de las comunicaciones*. Madrid: Civitas.
- Martínez de Pisón, J. (1997). *Derechos humanos: historia, fundamento y realidad*. Zaragoza: Egido.
- Martínez Martínez, R. (2004). *Una aproximación crítica a la autodeterminación informativa*. Madrid: Thomson-Civitas y APDCM.
- Martín-Retortillo Baquer, L. (Abril-Junio de 2009). La doble funcionalidad de la Ley Orgánica por la que autoriza la ratificación del Tratado de Lisboa (La Carta de Derechos Fundamentales de la Unión Europea en el "Boletín Oficial del Estado"). *Revista española de Derecho Europeo*(No. 30), 135-158.
- Mattelart, A. (2001). *Historia de la sociedad de la información*. (G. Multigner, Trad.) París: Le Découverte.
- Messia de la Cerda Ballesteros, J. A. (2004). *La protección de datos de carácter personal en las telecomunicaciones*. Madrid: Universidad Rey Juan Carlos.
- Moy, J. (2010). Beyond 'The Schoolhouse Gates' and into the Virtual Playground: Moderating Student Cyberbullying and Cyberharassment After "Morse v. Frederick". *Hastings constitutional law quarterly*, Vol. 37(Num. 3), 565-590.
- Muñoz Machado, S. (Febrero de 2010). La república del ciberespacio. *El Cronista del Estado Social y Democrático de Derecho*(No. 10), 78-90.
- Murillo de la Cueva, P. L. (2000). La comunicación de la Administración con los ciudadanos a través de Internet. En A. d. Datos, *Jornadas sobre protección de la privacidad. Telecomunicaciones e Internet. Pamplona, 22 y 23 de junio de 2000*. (pág. 81 a 98). Pamplona: Universidad Pública de Navarra.

- Murillo de la Cuenva, P. L. (2011). Observaciones sobre la privacidad del menor ante las nuevas tecnologías instrumentos jurídicos y competencia judicial. En J. L. Piñar Mañas, *Redes Sociales y Privacidad del Menor* (págs. 109-122). Madrid: Reus.
- Nava Gomar, S., Luna Pla, I., & Villanueva, E. (2006). *Derecho de acceso a la información pública parlamentaria*. México: H. Cámara de Diputados LIX Legislatura, Libertad de Información México A.C., Instituto Iberoamericano para el fortalecimiento del Poder Legislativo A.C. y Miguel Angel Porrúa.
- Nogueira Alcalá, H. (2000). El derecho a la información en el ámbito del Derecho Constitucional comparado en iberoamérica y Estados Unidos. En J. y. Carpizo, *Derecho a la información y derechos humanos. Estudios en homenaje al maestro Mario de la Cueva* (Vols. Serie Doctrina Jurídica, Núm. 37, págs. 3-143). México: Porrúa y Universidad Nacional Autónoma de México.
- Novoa Monreal, E. (2001). *Derecho a la privacidad y libertad de información* (6 ed.). Buenos Aires: Siglo XXI editores.
- Orwell, G. (2004). *1984* (Vol. 17). España: Destino.
- Pachot, K. (2010). A propósito del carácter fundamental de los derechos económicos, sociales y culturales. Una mirada desde la doctrina comparada y la experiencia del ordenamiento jurídico cubano. *Estudios Constitucionales. Revista semestral del Centro de Estudios Constitucionales de Chile*(Año 8, No. 1), 13-42.
- Padilla, M. M. (2001). *Bancos de datos y acción de hábeas data*. Buenos Aires: Abeledo-Parrot.
- Palomar Olmeda, A. (Enero-Junio de 2007). Los derechos personales en el ámbito de la protección de datos. *Revista española de protección de datos*(No.2), 9-40.

- Peces-Barba Martínez, G. (1982). *Tránsito a la modernidad y derechos fundamentales*. Madrid: Mezquita.
- Pegoraro, L., Coen, L., & Scarciglia, R. (2000). *Istituzioni di Diritto Pubblico e Diritto Costituzionale. Testi normativi* (2 ed.). Torino: G. Giappichelli editore.
- Peña Neira, S. (Mayo-Agosto de 1998). La noción de orden público y sus efectos en la regulación jurídica del comercio internacional en Chile. Especial atención a la aplicación de la Sentencia extranjera. *Revista de Derecho Privado*(Num. 26), 101-118.
- Perales, A. E. (2007). *Derecho al secreto de las comunicaciones*. Madrid: Iustel.
- Pérez Luño, A.-E. (1976). *Cibernética, informática y Derecho (un análisis metodológico)*. Bolonia: Publicaciones del Real Colegio de España.
- Pérez Luño, A.-E. (1996). *Manual de informática y Derecho*. Barcelona: Ariel.
- Pérez Luño, A.-E. (2005). *Derechos humanos, Estado de Derecho y Constitución* (9 ed.). Madrid: Tecnos.
- Pérez Luño, A.-E. (2006). *La tercera generación de derechos humanos*. Navarra: Aranzadi.
- Pi Llorens, M. (2001). *La Carta de los derechos fundamentales de la Unión Europea*. Barcelona: Publicacions de la Universitat de Barcelona.
- Pino, G. (2006). Il diritto all'identità personale ieri e oggi informazione, mercato, dati personali. En P. Cendon, *Libera circolazione e protezione dei dati personali*. Trattati, Tomo I (págs. 257-330). Milano: Giuffrè.
- Piñar Mañas, J. L. (2003). *Protección de datos de carácter personal en Iberoamérica (II Encuentro iberoamericano de protección de datos, la Antigua-Guatemala, 2-6 de junio de 2003)*. Valencia: Tirant lo blanch.
- Piñar Mañas, J. L. (2006). *La Red Iberoamericana de Protección de Datos. Declaraciones y documentos*. Valencia: Tirant lo blanch.

- Piñar Mañas, J. L. (2011). El derecho fundamental a la protección de datos y la privacidad de los menores en las redes sociales. En J. L. Piñar Mañas, *Redes Sociales y Privacidad del Menor* (págs. 61-84). Madrid: Reus.
- Piza R., R. E., & Trejos, G. (1989). *Derecho Internacional de los derechos humanos*. San José, Costa Rica: Juricentro.
- Puy, F. (1985a). *Derechos humanos* (Vols. 1. Derechos economicos, sociales y culturales). Santiago de Compostela: Paredes.
- Puy, F. (1985b). *Derechos humanos* (Vol. 2. Derechos civiles). Santiago de Compostela: Paredes.
- Puy, F. (1985c). *Derechos humanos*. (Vol. 3. Derechos políticos). Santiago de Compostela: Paredes.
- Quaranta, M. (2006). *Il Codice della Pubblica Amministrazione Digitale*. Napoli: Liguori.
- Quiroga Lavié, H. (2001). *Hábeas data*. Buenos Aires: Zavala.
- Rainer, A. (1998). La Declaración Universal de Derechos Humanos y su importancia para el desarrollo de la cultura del Derecho. En M. Balado, *La Declaración Universal de los Derechos Humanos en su 50 aniversario*. Barcelona: Bosch.
- Rebollo Delgado, L., & Serrano Pérez, M. M. (2006). *Introducción a la protección de datos*. Madrid: Dykinson.
- Revenge Sánchez, M. (1995). *El imperio de la política. Seguridad nacional y secreto de Estado en el sistema constitucional norteamericano*. Barcelona, España: Ariel.
- Ríos Estavillo, J. J. (2005). *Derecho a la información en México*. México: Porrúa.
- Rodríguez Padrón, C. (1999). La protección penal del domicilio. En E. Torres-Dulce Lifante, *Derecho al honor, a la intimidad y a la propia imagen II* (págs. 85-130). Madrid: Consejo General del Poder Judicial.

- Rodríguez Palop, M. E. (2002). *La nueva generación de derechos humanos. Origen y justificación*. Madrid: Dykinson y Universidad Carlos III de Madrid.
- Rodríguez Ruíz, B. (1998). *El secreto de las comunicaciones: tecnología e intimidad*. Madrid: McGraw-Hill.
- Ruiz de Querol, R., & Buirra, J. (2007). *La sociedad de la información*. Barcelona: UOC.
- Ruíz Miguel, C. (2004). *Estudio sobre la Carta de los derechos fundamentales de la Unión Europea*. Santiago de Compostela: Universidad de Santiago de Compostela.
- Saez Capel, J. (1999). *El derecho a la intimidad y las escuchas telefónicas*. Buenos Aires: Din Editora.
- Sancho Villa, D. (2003). *Transferencia internacional de datos personales*. Madrid: Agencia de Protección de Datos.
- Santamaría Ramos, F. J. (2011). *El encargado independiente. Figura clave para un nuevo Derecho de Protección de datos*. Madrid: La Ley.
- Sepúlveda Amor, B. (2002). *Terrorismo, seguridad nacional y seguridad colectiva*. México: Instituto de Investigación Económica y Social Lucas Alamán, A.C.
- Serrano Pérez, M. M. (2003). *El derecho fundamental a la protección de datos. Derecho español y comparado*. Madrid: Thomson-Civitas.
- Soares Martínez, P. (1978). *Comentários constituição portuguesa de 19*. Lisboa: Verbo.
- Suñé Llinás, E. (2002). *Tratado de Derecho Informático (2ª ed., Vol. I Introducción y protección de datos personales)*. Madrid: Servicio de Publicaciones de la Facultad de Derecho de la Universidad Complutense de Madrid e Instituto Español de Informática y Derecho.

- Suñé Llinás, E. (2009). Derecho Infromático, electrónico y de las comunicaciones. En E. Suñé Llinás, & F. Lara Yuste, Derecho Infromático, electrónico y de las comunicaciones. Actas de la IIª Convención Internacional de Derecho Informático (págs. 39-64). Madrid: Asociación Multisectorial de Empresas de Tecnologías de la Información, Comunicaciones y Electrónica (ASIMELEC) y Centro Internacional de Informática y Derecho (CIID).
- Troncoso Reigada, A. (2008). Transparencia administrativa y protección de datos personales. En A. Troncoso Reigada, *Transparencia administrativa y protección de datos personales. V Encuentro entre Agencias Autonómicas de Protección de Datos* (págs. 23-188). España: APDCM y Thomson-Civitas.
- Veleiro, B. (2008). *Protección de datos de carácter personal y sociedad de la información*. Madrid: Boletín Oficial del Estado.
- Verhellen, E. (2002). *La Convención sobre los derechos del niño. Trasfondo, motivos, estrategias, temas principales*. Leuven: Garant.
- Villanueva, E. (2003). *Derecho de acceso a la información pública en Latinoamérica. Estudio introductorio y compilación*. México, DF: Universidad Nacional Autónoma de México.
- Villanueva, E. (2006a). *Derecho de la información*. México: H. Cámara de Diputados LIX Legislatura, Universidad Nacional Autónoma de México, Instituto de Investigaciones Jurídicas y Miguel Angel Porrúa.
- Villanueva, E. (2006b). *Derecho de acceso a la información en el mundo*. México: H. Cámara de Diputados LIX Legislatura, Universidad Nacional Autónoma de México, Instituto de Investigaciones Jurídicas y Miguel Angel Porrúa.
- Villaseñor Goyzueta, C. A. (2011). *Proporcionalidad y límites de los derechos fundamentales. Teoría general y su reflejo en la jurisprudencia mexicana*.

México: Escuela Libre de Derecho, Porrúa y Universidad Complutense de Madrid.

Villaverde Menéndez, I. (2008). Publicidad registral y datos personales. Una especial mención al caso de los registros civil, de la propiedad y mercantil. En A. Troncoso Reigada, *Transparencia administrativa y protección de datos personales. V Encuentro entre Agencias Autonómicas de Protección de Datos Personales* (págs. 263-290). España: APCM y Thomson-Civitas.

Warren, S., & Brandeis, L. (1995). *Derecho a la intimidad (originalmente publicado como "The right to privacy" en Harvard Law Review, Vol. IV, nº. 5, pags. 193-219)*. (B. Pendás, & P. Baselga, Trads.) Madrid: Civitas.

2. Instrumentos internacionales o regionales

Acuerdo sobre asuntos jurídicos suscrito el 3 de enero de 1979 por la Santa Sede y el Estado español.

Carta de los Derechos Fundamentales de la Unión Europea.

Código Mundial Antidopaje.

Convención Americana sobre Derechos Humanos de 1969 (Pacto de San José).

Convención sobre los Derechos del Niño (20/11/1989).

Convenio Europeo de Derechos Humanos

Convenio No. 108 del Consejo de Europa, de 28 de enero, para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal.

Declaración Americana de los Derechos y Deberes del Hombre.

Declaración Universal de los Derechos Humanos de 1948.

Directiva 95/46/CE del Parlamento europeo y del Consejo, de 24 de octubre, 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.

Pacto Internacional de los Derechos Civiles y Políticos de 1966.

Reglamento (CE) nº 460/2004 del Parlamento Europeo y del Consejo, de 10 de marzo de 2004, por el que se crea la Agencia Europea de Seguridad de las Redes y de la Información.

3. Legislaciones nacionales

a) España

Código Civil

Código Penal

Constitución de España (06/12/1978).

LO 07/1980, de 5 de julio, de libertad religiosa.

LO 01/1982, de 5 de mayo, de protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen.

LO 02/1991, de 7 de enero, sobre derechos de información de los representantes de los trabajadores en materia de contratación.

LO 05/1992, de 29 de octubre, de Regulación del Tratamiento Automatizado de los Datos de carácter Personal (LORTAD).

LO 15/1999, de 13 de diciembre, de Protección de Datos de carácter Personal (LOPD).

LO 07/2006, de 21 de noviembre, de protección de la salud y de lucha contra el dopaje y el deporte.

Proyecto de Ley de transparencia, acceso a la información pública y buen gobierno en España, aprobado por el Consejo de Ministros el 17 de julio de 2012.

RD 1332/1994, de 20 de junio, por el que se desarrolla determinados aspectos de la Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal.

RD 424/2005, de 15 de abril, por el que se aprueba el Reglamento sobre las condiciones para la prestación de servicios de comunicaciones electrónicas, el servicio universal y la protección de los usuarios.

RD 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal.

b) México

Código Penal Federal.

Constitución Política de los Estados Unidos Mexicanos (05/02/1917).

Criterios Generales para la instrumentación de medidas compensatorias sin la autorización expresa del IFAI (DOF 18/04/2012)

Ley Federal de Protección de Datos Personales en posesión de particulares, de 27 de abril de 2010.

Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental, de 11 de junio de 2002.

Ley General de Cultura Física y Deporte, de 24 de feb de 2003.

Ley Orgánica de la Administración Pública Federal (DOF 14/06/2012).

Lineamientos de Protección de Datos Personales (27/07/2005).

Reglamento de la Ley Federal de Protección de Datos Personales en posesión de particulares.

c) Otras

Carta Magna de 1215 (Inglaterra).

Codice in materia di protezione dei dati personali, de 30 de junio de 2003 (Italia).

Constitución de Alemania (Ley Fundamental para la República Federal de Alemania, conocida como la Ley Fundamental de Bonn) (23/05/1949).

Constitución de Francia (V República) (04/10/1958).

Constitución de Portugal (02/04/1976).

Declaración de los Derechos del Hombre y del Ciudadano de 1789 (Francia).

Federal Data Protection Act (Ley Federal de Protección de Datos de Alemania) (15/11/06).

Ley 10/91, de 29 de abril (Portugal).

Ley 25.326 de Protección de Datos Personales, de 4 de octubre de 2000 (Argentina)

Ley 28/94, de 29 de agosto (Portugal).

Ley Federal de Protección de Datos Personales No. 67/98, de 26 de octubre (Portugal).

Loi 78-17 Informatique et Libertes (Ley 78/17 de informática y libertades de Francia) (06/01/1978).

4. Sentencias del Tribunal Europeo de Derechos Humanos

1. Peck Vs. Reino Unido.
2. L.L. Vs. Francia.

3. I. Vs. Finlandia.
4. S. y Marper Vs. Reino Unido.
5. Segerstedt-Wiberg y otros Vs. Suecia.
6. Amann Vs. Suiza.
7. Perry Vs. Reino Unido.
8. Henaf Vs. Francia de 27 de noviembre de 2003, relativa al encadenamiento en cama de un delincuente reincidente, sin antecedentes de violencia para que tal medida fuese tomada.
9. Tyrer Vs. Reino Unido de 25 de abril de 1978.
10. Saadi Vs. Reino Unido de 29 de Enero de 2008.
11. Irlanda Vs. Reino Unido, de 18 de enero de 1978.
12. STEDH de 9 de febrero de 1967, en el caso del régimen lingüístico de la enseñanza en Bélgica.
13. Dudgeon Vs. el Reino Unido de 22 de octubre de 1981.
14. Norris Vs. Irlanda de 26 de octubre de 1988.
15. Modinos Vs. Chipre de 22 de abril de 1993.
16. A.D. T. Vs. el Reino Unido de 31 de Julio de 2000.
17. L y V Vs. Austria, de 9 de enero de 2003.
18. S.L Vs. Austria, de 9 de enero de 2003.
19. Smith y Grady Vs. el Reino Unido, de 27 de septiembre de 1999.
20. Lusting-Perean y Beckett Vs. el Reino Unido de 27 de septiembre de 1999.
21. Perkins y R. Vs. el Reino Unido de 22 de octubre de 2002.
22. Beck, Copp, y Bazeley Vs. el Reino Unido de 22 de octubre de 2002.
23. I Vs. Reino Unido, de 11 de julio del 2002.
24. Christine Goodwin Vs. el Reino Unido, de 11 de julio del 2002.
25. Van Kück Vs. Alemania de 12 de junio de 2003.
26. Caso Klass num. 55.
27. Caso Leander de 26 de marzo de 1987.
28. Caso Z de 25 de febrero de 1997.

29. Caso Funke de 25 de febrero de 1993.

31. Caso Gaskin de 7 de julio de 1999.

30. Caso X e Y de 26 de marzo de 1985.

5. Sentencias del Tribunal Constitucional

STC 033/1982, de 8 de junio.

STC 099/1994, de 11 de abril

STC 022/1984, de 17 de febrero.

STC 143/1994, de 09 de mayo.

STC 083/1984, de 24 de julio.

STC 011/1998, de 13 de enero.

STC 110/1984, de 26 de noviembre.

STC 094/1998, de 04 de mayo.

STC 117/1984, de 5 de diciembre.

STC 018/1999, de 22 de febrero.

STC 106/1986, de 24 de julio.

STC 049/1999, de 05 de abril.

STC 137/1986, de 06 de noviembre.

STC 144/1999, de 22 de julio.

STC 159/1986, de 16 de diciembre.

STC 180/1999, de 11 de octubre.

STC 196/1987, de 11 de diciembre.

STC 202/1999, de 08 de noviembre.

STC 070/1987, de 30 de octubre.

STC 290/2000, de 30 de noviembre.

STC 144/1987, de 23 de septiembre.

STC 292/2000, de 30 de noviembre.

STC 170/1987, de 30 de octubre.

STC 297/2000, de 11 de diciembre.

STC 231/1988, de 01 de diciembre.

STC 049/2001, de 26 de febrero.

STC 214/1991, de 11 de noviembre.

STC 081/2001, de 26 de marzo.

STC 219/1992, de 03 de diciembre.

STC 156/2001, de 12 de junio.

STC 142/1993, de 22 de abril.

STC 119/2001, de 02 de julio.

STC 254/1993, de 20 de julio.

STC 186/2001, de 17 de septiembre.

STC 057/1994, de 28 de febrero.

STC 216/2006, de 03 de julio.

STC 254/1994, de 15 de septiembre

STC 023/2010, de 27 de abril.

6. Autos del Tribunal Constitucional

ATC 030/1989, de 5 de junio.

ATC 020/2011, de 28 de febrero

ATC 462/1996

ATC 300/1989

7. Sentencias de la Audiencia Nacional

SAN 029/2006, de 9 de febrero

SAN, Sección 1ª, de 16 de enero de 2008 (rec.) relativa a los libros bautismales.

SAN, Sección 1ª, de 18 de enero de 2002 (rec. 924/2000).

SAN, Sección 1ª, de 14 de junio de 2002 (rec. 650/2001).

SAN, Sección 1ª, de 15 de noviembre de 2002 (rec. 732/2002).

SAN, Sección 1ª, de 9 de noviembre de 2005 (rec. 371/2003).

SAN, Sección 1ª, de 3 de noviembre de 2004 (rec. 1160/2002).

SAN, Sección 1ª, de 25 de enero de 2006 (rec. 227/2004).

SAN, Sección 1ª, de 10 de noviembre de 2006 (rec. 119/2005).

SAN, Sección 1ª, de 23 de marzo de 2006 (rec. 478/2004).

SAN, Sección 1ª, de 15 de octubre de 2003 (rec. 1517/2001).

8. Diccionarios y enciclopedias

Diccionario de la Real Academia Española.

Enciclopedia Jurídica Omeba. Versión digital, 2005.

9. Boletines y diarios oficiales

Boletín Oficial (Argentina).

Boletín Oficial del Estado (España).

Diario Oficial de la Federación (México).

10. Otras fuentes

Boletín de Jurisprudencia Constitucional, No. 33, de enero de 1984, Sentencia del Tribunal Constitucional alemán, publicado por las Cortes Generales, en Madrid, Traducción de Manuel Daranas.

Boletín de Jurisprudencia Constitucional, No. 83, 1984.

Decisión del Consejo Europeo, relativa a la elaboración de una Carta de Derechos Fundamentales de la Unión Europea, anexo 4 de las conclusiones de la Presidencia del Consejo Europeo de Colonia, celebrado los días 3 y 4 de junio de 1999. Boletín de la Unión Europea No. 6/1999.

Opinión consultiva de la Corte OC-2/82 de 24 de septiembre de 1982, relativa al efecto de las reservas sobre la entrada en vigencia de la Convención Americana sobre Derechos Humanos, solicitada por la Comisión Interamericana de Derechos Humanos.

Anexos. Resoluciones del IFAI de protección de datos personales

El derecho a la protección de datos personales, como se ha visto, ha evolucionado en México, tan es así que hoy lo vemos reflejado en los arts. 6, 16 y 73.XXIX-O CPM. Sin embargo, con anterioridad a este hecho, el Instituto Federal de Acceso a la Información Pública hubo de resolver casos en donde la controversia principal era la publicidad o no de datos personales solicitados al sujeto obligado. Es así que en este apartado, describiendo resoluciones emitidas por el Instituto Federal de Acceso a la Información Pública, veremos el extracto de algunos casos que el Instituto ha resuelto con relación al derecho de protección de datos personales en México.

Resolución 676/2005, de 17 de agosto

Número de expediente: 676/05. Recurrente: Bernardo Salas Mar. Ponente: María Marván Lobarde. Dependencia ante la que se presentó la solicitud: Comisión Federal de Electricidad. Resolución de fecha: 17 de Agosto de 2005.

En el presente caso, la **petición** del recurrente a la Comisión Federal de Electricidad (CFE) fueron los Permisos de Trabajo en Áreas con Radicación PETAR 96/1E-511 y PETAR 96/1E-534 correspondientes a los trabajos realizados en la Alberca de Supresión de la Central Nuclear Laguna Verde en 1996.

En su **respuesta**, la CFE señaló al recurrente que dado el volumen de la información, no era posible la transferencia vía electrónica y que la información consistía en lo siguiente:

“La información proporcionada por la Comisión Federal de Electricidad consiste de:

PETAR No. 96/IE511.- Integrado por una hoja de portada y 28 hojas complementarias, con vigencia del 7 al 31 de octubre de 1996.

PETAR No. 96/IE534.- Integrado por una hoja de portada y 39 hojas complementarias, con vigencia del 10 al 27 de octubre de 1996.

Cabe aclarar que la numeración en la esquina inferior derecha de las hojas presenta discontinuidades que corresponden a los registros detallados de dosis individuales por cada entrada a la zona de trabajo, los cuales no fueron incluidos por tratarse de información que no puede ser liberada sin autorización expresa de las personas ahí registradas, con fundamento en los artículos 3, fracción II y 21, de la Ley Federal de

Transparencia y Acceso a la Información Pública Gubernamental. Sin embargo, se hace la acotación de que para el PETAR No. 96/IE511 las dosis individuales máximas y promedio fueron de 387 y 78 mrem³¹⁷ respectivamente, y que para el PETAR No. 96/IE534 dichos valores fueron de 878 y 324 mrem. Como valor de referencia, el límite de dosis individual en el año (1996) era de 1250 mrem por trimestre”.

La CFE al dar respuesta señaló que estaba otorgando acceso a una versión pública de la información requerida³¹⁸. Al respecto, el Reglamento General de Seguridad Radiológica, que tiene por objeto proveer en la esfera administrativa a la observancia de la Ley Reglamentaria del Artículo 27 Constitucional en Materia Nuclear en lo relativo a seguridad radiológica, en su artículo 6 define como personal ocupacionalmente expuesto aquel que en ejercicio y con motivo de su ocupación está expuesto a radiación ionizante o a la incorporación de material radiactivo.

El recurrente **impugnó** la citada respuesta señalando que la información entregada era incompleta, pues aunque revelaba sobreexposición a la radiación de los trabajadores, era necesario saber las dosis recibidas por cada uno de esos trabajadores. Anexando además una hoja con la información completa, en donde el recurrente muestra al Instituto las omisiones de la CFE en su respuesta.

Por lo anterior el IFAI procedió a analizar si la clasificación de la información efectuada por el órgano desconcentrado se ha efectuado conforme a lo dispuesto por la Ley, considerando si dentro de los permisos de trabajo en áreas con radiación de referencia existe información relativa a datos personales.

La CFE en sus **alegatos** manifestó que las dosis de radiación recibidas por cada trabajador de la Central Nuclear Laguna Verde (CNLV) se referían a información que correspondía a datos personales de los trabajadores, por lo que era confidencial y se necesitaba del consentimiento expreso de sus titulares para

³¹⁷ El milirem (abreviación mrem) es la unidad utilizada para medir el efecto de la radiación en el cuerpo humano. El milirem es una cantidad muy pequeña de la radiación.

³¹⁸ Esto lo refiere de la siguiente manera: “Cabe aclarar que la numeración en la esquina inferior derecha de las hojas presenta discontinuidades que corresponden a los registros detallados de dosis individuales por cada entrada a la zona de trabajo, los cuales no fueron incluidos por tratarse de información que no puede ser liberada sin autorización expresa de las personas ahí registradas, con fundamento en los artículos 3, fracción II y 21, de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental”.

proporcionarla. Agregando además, que las dosis que cada uno de los trabajadores recibían pasaban a formar parte de su expediente personal auditable³¹⁹.

En este orden de ideas, el Instituto señaló que la información que fue omitida en la versión pública otorgada al recurrente formaba parte del historial dosimétrico del personal ocupacionalmente expuesto, correspondiente a los permisos de trabajo en áreas con radicación PETAR 96/1E-511 y PETAR 96/1E-534 relativos a los trabajos realizados en la Alberca de Supresión de la Central Nuclear Laguna Verde en 1996. De esta forma, el Reglamento General de Seguridad Radiológica establece que las dosis recibidas a consecuencia de la exposición a fuentes de radiación ionizante y de prácticas que entrañan la irradiación con radiación ionizante o incorporación de material radiactivo, se sujetarán a un sistema de limitación de dosis que tiene como finalidad *evitar los efectos no estocásticos y limitar la ocurrencia de los estocásticos a un nivel aceptable*, por lo que se establecen límites para cada caso, debiendo aplicarse el que resulte más restrictivo para el órgano o tejido irradiado.

De acuerdo con el artículo 9 del Reglamento General de Seguridad Radiológica, los *efectos no estocásticos* son aquellos en los que la severidad del efecto es función de la dosis y se presentan a partir de un valor umbral -dosis umbral es el valor de la dosis por debajo del cual se considera que un efecto no estocástico determinado no se manifestará-. Estos efectos se presentan en el individuo expuesto. Los *efectos estocásticos* son aquellos en los que la probabilidad de que el efecto se presente, se considera como una función de la dosis, sin que exista una dosis umbral y pueden manifestarse tanto en el individuo expuesto como en su descendencia.

Como se desprende de lo anterior, la información relativa a las dosis individuales que recibieron los trabajadores se ubica en lo señalado por el artículo 3 fracción II de la Ley Federal de Transparencia y Acceso a la Información Pública

³¹⁹ En términos del artículo 6 del Reglamento General de Seguridad Radiológica, la radiación ionizante es toda radiación electromagnética o corpuscular capaz de producir iones, directa o indirectamente, debido a su interacción con la materia. El artículo 160 fracciones X, XI y XII del citado Reglamento, establece entre las obligaciones del personal ocupacionalmente expuesto el enterarse de los equivalentes de dosis que ha recibido en el desempeño de sus labores con la periodicidad con que se anoten en el registro correspondiente, el someterse a la toma de muestras biológicas que se requieran para la vigilancia médica y para las pruebas de bioensayo, así como proporcionar con veracidad los datos que le sean requeridos durante las inspecciones, auditorías, verificaciones y reconocimientos que realice la Comisión.

Gubernamental, ya que se trata de información a partir de la cual se puede llegar a conocer cuál es el estado de salud del personal ocupacionalmente expuesto; es decir, de acuerdo con lo señalado en los párrafos precedentes existe una relación directa entre las dosis de radiación a las que se encuentra expuesta una persona y los efectos que se producirán en esa persona ya sean positivos, negativos o bien, que no alteren el estado que guarda, reflejando en todos los casos el estado físico de dichos sujetos. Sin embargo, al otorgar la CFE un listado innominado de la exposición a radiación, no se estarían revelando datos personales, pues no existiría vínculo directo entre la dosis de radiación recibida con el nombre del servidor público expuesto.

Por lo anterior, el IFAI **modificó** la resolución de la Comisión Federal de Electricidad instruyéndole para que entregara un listado innominado sobre las dosis recibidas por sus trabajadores en el periodo solicitado. Añadiendo que se procedería otorgar acceso a la información omitida en la versión pública, esto es, a los registros en los que se contienen los niveles de dosis a que fueron expuestos los trabajadores en lo individual, únicamente a su titular, previa acreditación de la identidad o personalidad de su representante legal.

Resolución 932/2005, de 11 de junio

Número de expediente: 932/05. Recurrente: José Carlos Campos Riojas
Ponente: Horacio Aguilar Álvarez de Alba. Dependencia ante la que se presentó la solicitud: Fondo de Garantía y Fomento para la Agricultura, Ganadería y Avicultura. Resolución de fecha: 11 de Junio de 2003.

En el presente caso, la **petición** de la recurrente, fue requerir todos los datos de los empleados del sujeto obligado, particularmente los siguientes: 1. Nombre completo; 2. Profesión; 3. Fotografía; 4. Currículo; 5. Fecha de nacimiento; 6. Puesto; 7. Nivel de ingreso –por categoría y salario bruto y neto—; 8. Jefe inmediato; 9. Subordinados inmediatos; 10. Fecha de ingreso a la dependencia; 11. Dirección y teléfonos de su oficina y 12. Correo electrónico asignado; 13. Número de teléfono celular –en caso de que sea pagado por la Secretaría- y; 14. Teléfono de fax.

A dicha solicitud, el sujeto obligado en su **respuesta**, puso a disposición del recurrente la información solicitada relativa al nombre completo, profesión, fecha de nacimiento, puesto, nivel de ingreso –por categoría y salario bruto y neto-, jefe inmediato, fecha de ingreso a la dependencia, dirección y teléfonos de su oficina, correo electrónico asignado y teléfono de fax.

La recurrente presentó **recurso de revisión** ante este Instituto, manifestando su inconformidad a la negativa del sujeto obligado de entregar algunos datos (número de teléfono celular –en caso de que sea pagado por la Secretaría-, currículo y subordinados inmediatos) por considerarlos reservados y confidenciales. Por tanto, el presente recurso de revisión tendría por objeto determinar la procedencia de la clasificación realizada por el Fondo de Garantía y Fomento para la Agricultura, Ganadería y Avicultura respecto a dichos datos.

En sus **alegatos**, el sujeto obligado manifestó que por lo que respecta a los **números de teléfono celular asignados a determinados servidores públicos**, se encuentra impedido para otorgar dicha información de conformidad con lo que establecen los artículos 19, 20 y 21 de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental, por considerarse información **confidencial**, cuya entrega causaría el entorpecimiento en el desarrollo de las funciones encomendadas a sus propios funcionarios, pudiendo causar serios perjuicios a la propia Institución dada la importancia de dichas actividades, además de que se estaría contraviniendo lo estipulado en el artículo 13 fracción IV de la Ley, toda vez que el teléfono celular que se asigna a los funcionarios se hace precisamente con el fin de localizarlos en cualquier momento y en cualquier lugar, lo cual provocaría una violación a su intimidad.

Las fracciones III y IV del artículo 7 de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental, respectivamente señalan que los sujetos obligados deberán *poner a disposición del público a través de Internet, información actualizada relativa al directorio de servidores públicos, desde el nivel de jefe de departamento o sus equivalentes, así como la remuneración mensual por puesto*. Así también, el artículo 13 del Reglamento de la Ley señala que el directorio de servidores públicos debe incluir el *nombre, cargo, nivel del puesto en la estructura orgánica, número telefónico, domicilio para recibir*

correspondencia y, en caso de contar con ellos, el *número de fax* y la *dirección electrónica*. Así mismo, el artículo 14 del Reglamento indica que en lo relativo a la información sobre las *remuneraciones de los servidores públicos*, se debe publicar el tabulador y las compensaciones brutas y netas, así como las prestaciones correspondientes *del personal de base, de confianza y del contratado por honorarios*.

Por lo que, se desprende que la información de los servidores públicos que se encuentra íntimamente relacionada con el desempeño de su encargo, así como aquella que le *permite a los sujetos obligados presentar una adecuada rendición de cuentas, tiene el carácter de pública*. La Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental, obliga a la publicidad del número telefónico, número de fax y dirección electrónica de los servidores públicos que laboran en las dependencias o entidades. La *ratio legis* del legislador radica en permitir a la ciudadanía tener un acceso expedito a aquellas personas que ocupan algún cargo en el servicio público del gobierno federal.

El legislador fue claro al precisar que los números telefónicos de todos los individuos, incluyendo el de los servidores públicos en tanto que son personas privadas, constituyen datos personales en términos del artículo 3, fracción II, de la Ley de la materia, pues ellos corresponden única y exclusivamente al ámbito privado de su vida y por ende, a su intimidad. Además que la Ley no distingue entre aquellos teléfonos correspondientes a las oficinas de los servidores públicos y los números de telefonía celular; por lo que *“si la ley no distingue, no se debe distinguir”*, además que dentro del concepto de “número de teléfono” se encuentra el número de teléfono celular.

Sin embargo, el **Instituto** refiere que sólo ciertos servidores públicos tenían derecho a la asignación de un **teléfono celular** y que ello correspondía a una prestación denominada “beneficio inherente al puesto”, **para coadyuvar al mejor desempeño de las funciones de los servidores públicos**³²⁰. Y que además, la función principal del teléfono celular era la de proporcionarle al servidor público

³²⁰ El Anexo “D” del Manual de Percepciones de la Administración Pública Federal, publicado en el Diario Oficial de la Federación el 31 de Marzo del 2005, precisa que los beneficiados por esta prestación serán solamente los servidores públicos que ocupen los cargos de Secretario de Estado, Subsecretario de Estado, Oficial Mayor, Jefe de Unidad, Director General y Coordinador General (en su defecto el Titular de la Entidad).

que lo utiliza, un instrumento eficaz que pudiera comunicarlo no sólo con su centro de trabajo, sino también con otras personas en ejercicio de sus funciones. Por tanto, el equipo de telefonía celular que se le proporcionaba a un servidor público como parte de las prestaciones correspondientes a su cargo, era **información pública**, toda vez que era pagada con recursos del erario público. Añadiendo, que en modo alguno se afectaba a la intimidad del funcionario público con la publicidad de su teléfono celular, pues en el goce y disfrute de la privacidad bastaba con apagar el instrumento que coadyuvaba al desempeño de la responsabilidad pública, precisamente porque no se estaba desempeñando dicha responsabilidad.

En lo que respecta al **currículum vitae**, el sujeto obligado en su escrito de **alegatos** manifestó que era información clasificada como **reservada y confidencial**, por contener datos personales, que afectaban la intimidad de la persona, y por lo tanto, se requería del consentimiento de los individuos para su difusión, lo anterior con fundamento en el artículo 18 fracción II de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental.

En estos términos, el *currículum vitae* sí contiene datos personales, pues generalmente en él se señalan, al menos, el nombre de la persona, su domicilio, sus números telefónicos, su correo electrónico, su escolaridad y su experiencia laboral. Por tanto, en términos generales se trata de información que incide en la intimidad de un individuo identificado o identificable. No obstante ello, la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental prevé la publicidad obligatoria de ciertos datos relativos a los servidores públicos, en razón del cargo público que ocupan³²¹.

En este sentido, el Instituto concluyó que cierta información contenida en el currículum de un servidor público -contrario a lo que ocurre con el resto de las personas- era de naturaleza pública, toda vez que la misma acreditaba la idoneidad del servidor público de que se trate al cargo que ocupa.

³²¹ El artículo 7 de la Ley establece que los sujetos obligados deberán poner a disposición del público a través de internet, la información relativa al directorio de servidores públicos, desde el nivel de jefe de departamento o sus equivalentes (fracción III) y la remuneración mensual del puesto (fracción IV). El artículo 13 del Reglamento de la Ley señala que el directorio de los servidores públicos deberá incluir el nombre, cargo, nivel del puesto en la estructura orgánica, número de teléfono, domicilio para recibir correspondencia y, en caso de contar con ellos, el número de fax y la dirección electrónica.

El Registro de Servidores Públicos que lleva la Secretaría de la Función Pública contiene, entre otra, información relativa a los datos curriculares de los servidores públicos, así como a su situación patrimonial. Tratándose de la situación patrimonial, el artículo 40 de la Ley Federal de Responsabilidades Administrativas de los Servicios Públicos establece que dicha información será pública siempre y cuando se cuente con la autorización específica del servidor público de que se trate³²². Por tanto, al haberse precisado de manera específica que sólo se requiere del consentimiento del servidor público para difundir los datos relativos a su situación patrimonial, el resto de la información que consta en el Registro es de carácter público, ya que acredita la idoneidad del servidor público para el cargo que ocupa.

Por lo tanto, en esta resolución el Instituto apunta que se puede concluir que los **“datos curriculares”** que constan en el Registro referido al inicio del párrafo anterior, **no pueden ser considerados como confidenciales** con fundamento en el artículo 18, fracción II, de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental. Además nos dice que es importante aclarar que “datos curriculares” no es lo mismo que *currículum vitae*, pues los primeros son partes integrantes de este último sin constituirse como el currículum en su totalidad. Los “datos curriculares” a los que hace referencia el artículo 40 de la Ley Federal de Responsabilidades de los Servidores Públicos (www.servidorespublicos.gob.mx), son los siguientes: a) Grado máximo de estudios (nivel, institución educativa, carrera, estatus, entre otros); b) Experiencia laboral, tanto en el sector público como en el privado; c) Logros laborales o académicos, en su caso y; d) Experiencia académica, en su caso. Bajo ese tenor, los “datos curriculares” que por disposición legal son públicos no podrían considerarse confidenciales, por lo que la parte correspondiente del *currículum vitae* de un servidor público en el que consten tales datos, también es pública. En este sentido,

³²² El artículo 40 de la Ley Federal de Responsabilidades Administrativas de los Servicios Públicos establece que “La Secretaría llevará un registro de servidores públicos, el cual tendrá el carácter de público. En el registro se inscribirán los datos curriculares de los servidores públicos obligados a presentar declaración de situación patrimonial, sus funciones, ingresos y reconocimientos con motivo de sus empleos, cargos o comisiones; la información relativa a su situación patrimonial, en lo referente a sus ingresos del último año, bienes muebles e inmuebles, inversiones financieras y adeudos, así como en su caso los procedimientos administrativos instaurados y las sanciones impuestas a aquellos. La publicitación de la información relativa a la situación patrimonial, se hará siempre y cuando se cuente con la autorización previa y específica del servidor público de que se trate. ...”

y dado que el currículum vitae de un servidor público contiene tanto información pública como confidencial, el IFAI procedió a instruir al sujeto obligado para elaborar versiones públicas del currículum vitae, las cuales no podrían omitir los datos curriculares a que se refiere el mencionado artículo 40³²³.

En lo concerniente a la solicitud de los **nombres de los subordinados** inmediatos del personal hasta el nivel de subdirector, el sujeto obligado contestó que dicha lista se encuentra en la base de datos del Sistema de Recursos humanos y que es considerada como información reservada. A lo que el Instituto refirió que el artículo 7 fracciones I y III de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental, establece que los sujetos obligados deberán **poner a disposición del público su estructura orgánica y el directorio de servidores públicos**, desde el nivel de jefe de departamento o sus equivalentes. Además que el artículo 13 del Reglamento de la citada Ley, señala que en el mencionado directorio se deberá incluir el nombre, cargo, nivel de puesto en la estructura orgánica, número telefónico, domicilio para recibir correspondencia y, en caso de contar con ellos, el número de fax y la dirección electrónica³²⁴.

En este sentido, el espíritu del artículo 7 de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental y sus correlativos del Reglamento es poner a disposición del público la información relativa a la estructura orgánica y directorio de los servidores públicos, independientemente de que no sea obligación de transparencia publicar en Internet el directorio de la totalidad del personal que labora en la dependencia o entidad. Esto es, nada impide que los interesados tengan acceso a información que por definición legal y reglamentaria es pública, aun cuando no sea obligación publicarla en Internet, siempre que la misma se encuentre en posesión de los sujetos obligados.

De los razonamientos anteriores es como el Instituto concluyó **revocar** la clasificación realizada por el Fondo de Garantía y Fomento para la Agricultura, Ganadería y Avicultura, en los términos que hemos resumido de esta resolución.

³²³ Estos datos curriculares, serían el “mínimo” de información que debería entregarse al recurrente en las versiones públicas que elaborara el sujeto obligado de los currículum vitae solicitados.

³²⁴ Hay que distinguir entre la información que los sujetos obligados ponen a disposición del público por ministerio de Ley y sin que medie solicitud alguna, y las solicitudes de acceso a información que formulan los particulares que deben ser respondidas por los sujetos obligados de conformidad con lo establecido por la Ley.

Resolución 1659/2005, de 23 de noviembre

Número de expediente: 1659/05. Recurrente: M. Marcial Pérez y Pérez. Ponente: Alonso Lujambio Irazábal. Dependencia ante la que se presentó la solicitud: Instituto Nacional de Ciencias Médicas y Nutrición Salvador Zubirán. Resolución de fecha: 23 de Noviembre de 2005.

En el presente caso, la **petición** del recurrente a la al Instituto Nacional de Ciencias Médicas y Nutrición Salvador Zubirán, fue el requerimiento de “todas las cartas de consentimiento y autorización firmadas por las 45 mujeres saludables esterilizadas entre 29 y 35 años con ciclos menstruales regulares participantes en el estudio de investigación científica aprobado por el Comité Científico y de Ética Humana del Instituto Nacional de Ciencias Médicas y Nutrición Salvador Zubirán denominado: On the Mechanisms of Action on Short-Term Levonorgestrel Administration in Emergency Contraception”.

El Instituto Nacional de Ciencias Médicas y Nutrición Salvador Zubirán, dentro de su **respuesta** le informó al hoy recurrente que no podía entregarle la información solicitada por estar clasificada como confidencial por contener datos personales y médicos de las pacientes, ello con fundamento en el artículo 18 de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental. Finalmente, manifestó que el daño que causaría la difusión de la información solicitada sería identificar a las personas que participaron en el estudio. En su **recurso de revisión**, el recurrente se inconformó con la negativa del Instituto Nacional de Ciencias Médicas y Nutrición Salvador Zubirán. Manifestó además que, se estaba violando su derecho al acceso a la información al negarle información sobre una investigación que ya ha aparecido publicada en varias revistas, máxime que dicho estudio fue realizado en un Instituto de investigación nacional, al servicio de los mexicanos y pagado por estos.

En su escrito de **alegatos** el Instituto Nacional de Ciencias Médicas y Nutrición Salvador Zubirán reiteró la clasificación de la información con fundamento en el artículo 18 de la Ley; agregando que se reconocía el derecho de las personas a conocer el resultado de los trabajos de investigación realizados con fondos públicos y con la participación del mismo Instituto. Argumentando que el trabajo en cuestión fue publicado y podía ser consultado por cualquier persona, es

decir, es información pública, sin embargo lo anterior no incluía los datos personales de los participantes en éste u otros estudios de investigación biomédica. Posteriormente, el Comisionado Ponente solicitó al Instituto Nacional de Ciencias Médicas y Nutrición Salvador Zubirán, un alcance a sus alegatos en donde se especificaran detalladamente los datos que se omitirían en una versión pública de las cartas de consentimiento de las 45 mujeres.

En un **alcance a sus alegatos**, el Instituto Nacional de Ciencias Médicas y Nutrición Salvador Zubirán manifestó que el principio básico 22 de la *Declaración de Helsinki* señala que una vez que el individuo ha comprendido la información que se le ha proporcionado respecto a la investigación, "el médico debe obtener entonces, preferiblemente por escrito, el consentimiento informado y voluntario de la persona", a la vez que el principio 6 de la misma Declaración dice que "siempre se debe respetar el derecho del sujeto de investigación a salvaguardar su integridad. Deben tomarse todas las precauciones para respetar la privacidad del sujeto y minimizar el impacto del estudio sobre su integridad física y mental y sobre su personalidad"³²⁵.

Por otro lado, manifestó que en la versión más reciente de los Lineamientos Éticos para la Investigación Biomédica en la que participan Seres Humanos, el Lineamiento 18 denominado "Salvaguardando la Confidencialidad" establece que "el investigador debe establecer salvaguardas seguras de la confidencialidad de los sujetos de la investigación...".

Por su parte, el Artículo 9 de la Declaración Universal sobre Bioética y Derechos Humanos señala que "se debe respetar la privacidad de las personas interesadas y la confidencialidad de la información que les atañe. En la mayor medida posible esa información no debe utilizarse o revelarse para fines distintos de aquellos para los que se recopiló o para los que se obtuvo el consentimiento...".

³²⁵ Dentro de su alcance de alegatos, el Instituto Zubirán refirió que entre los instrumentos internacionales sobre el tema destacan la Declaración de Helsinki de la Asociación Médica Mundial, la recientemente adoptada Declaración Universal sobre Bioética y Derechos Humanos (de 19 de Octubre de 2005) y, los Lineamientos Éticos para la Investigación Biomédica en la que participan Seres Humanos. Todos esos documentos coinciden en que sólo debe involucrarse en investigaciones a aquellos individuos que otorguen su consentimiento voluntario e informado para ello, así como en que los intereses y el bienestar de la persona deben tener prioridad con respecto al interés exclusivo de la ciencia o la sociedad.

Además, el Instituto Nacional de Ciencias Médicas y Nutrición Salvador Zubirán manifestó que el marco jurídico de nuestro país se guía a su vez por los mismos principios que los instrumentos internacionales; particularmente, los principios de la Declaración de Helsinki, los cuales se encuentran reflejados en la Ley General de Salud y en su Reglamento en Materia de Investigación para la Salud. Es así que de conformidad con la fracción IV del artículo 100 de la Ley General de Salud, el consentimiento libre e informado para participar en proyectos de investigación científica es otorgado voluntariamente por las personas a través de la carta correspondiente, después de haber sido informadas sobre los objetivos, procedimientos, riesgos y beneficios que conlleva la investigación. Por su parte, el Reglamento de la Ley General de Salud artículo 16 señala que "en las investigaciones en seres humanos se protegerá la privacidad del individuo sujeto de investigación, identificándolo sólo cuando los resultados lo requieran y éste los autorice", a la vez que en su artículo 21, fracción VIII, establece que para que el consentimiento informado se considere existente deberá proporcionarse al sujeto de la investigación información sobre "la seguridad de que no se identificará al sujeto y que se mantendrá la confidencialidad de la información relacionada con su privacidad". El citado Instituto Zubirán señaló además que la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental reconoce como información reservada y confidencial aquella cuya difusión pueda poner en riesgo la vida, la seguridad o la salud de cualquier persona y los datos personales que requieran el consentimiento de los individuos para su difusión. Finalmente el Instituto de Ciencias Médicas y Nutrición Salvador Zubirán informó que para el desarrollo de la investigación en comento se utilizaron dos formatos distintos de carta de consentimiento, en ese tenor, el referido Instituto anexó a consideración del IFAI dos proyectos de versiones públicas para su entrega al recurrente.

El Instituto Federal de Acceso a la Información Pública consideró que el objeto de la presente resolución sería determinar la procedencia de dichas versiones públicas a la luz de las normas contenidas en la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental. En este sentido, el IFAI señaló que en el presente caso, estaba indiscutiblemente ante una solicitud de información de documentación que contenía datos personales, como lo era el consentimiento y

la participación de una persona en un proyecto de investigación científica³²⁶. Agregando que, resultaba incontrovertible que la decisión de participar en un proyecto de investigación científica constituía información que afecta la intimidad de las personas, no sólo por el hecho de que se trataba de una decisión voluntaria y, consecuentemente, personalísima, sino porque el hecho mismo de participar en este u otro proyecto de investigación *revelaba características físicas de las personas* que constituían requisitos para participar en el mismo, como en la especie, *el hecho de ser mujeres esterilizadas*.

Sin embargo, la documentación solicitada también contenía información que permitía la rendición de cuentas a los ciudadanos por parte de los sujetos obligados puesto que, para participar en proyectos de investigación científica, es obligación legal contar con el consentimiento previo, voluntario e informado de las personas, en términos del artículo 100, fracción IV de la Ley General de Salud. Siendo así que en el presente caso se encontraban dos de los objetivos señalados en el artículo 4 de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental que el IFAI debía armonizar: por un lado, garantizar la protección de datos personales en posesión de los sujetos obligados y, por el otro, favorecer la rendición de cuentas a los ciudadanos, de manera que puedan valorar el desempeño de los sujetos obligados.

Es en este contexto que el Instituto consideró que una versión pública de la documentación solicitada en la que se omitan todos aquellos datos que permitiesen identificar bajo cualquier circunstancia a las participantes en el proyecto de investigación científica, en términos de lo dispuesto en el segundo párrafo del artículo 43 de la Ley, persigue la armonización de los dos objetivos arriba citados.

Tercero. El Instituto Nacional de Ciencias Médicas y Nutrición Salvador Zubirán manifestó que para las cartas de consentimiento informado utilizó dos

³²⁶ Refiriendo que en términos de lo dispuesto en el artículo 3 fracción II de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental, los datos personales son toda información concerniente a una persona física, identificada o identificable, entre otra, la relativa a su origen étnico o racial, o que esté referida a las características físicas, morales o emocionales, a su vida afectiva y familiar, domicilio, número telefónico, patrimonio, ideología y opiniones políticas, creencias o convicciones religiosas o filosóficas, los estados de salud físicos o mentales, las preferencias sexuales, u otras análogas que afecten su intimidad.

formatos de carta, por lo que mandó dos proyectos de versiones públicas. Los elementos que eliminó en cada formato son los siguientes:

Formato 1:

1. Código numérico de identificación proporcionado por el Instituto Nacional de Ciencias Médicas y Nutrición Salvador Zubirán.
2. Nombre del investigador en contacto directo con la persona.
3. Nombre de la unidad en donde se realizó la investigación.
4. Teléfono del investigador.
5. Firma de la participante.
6. Firma del investigador principal.
7. Firmas de los testigos.

Formato 2:

1. Código numérico de identificación proporcionado por el Instituto Nacional de Ciencias Médicas y Nutrición Salvador Zubirán.
2. Nombre del investigador en contacto directo con la persona.
3. Número del proyecto (este dato no aparece en el formato 1).
4. Nombre de la unidad en donde se realizó la investigación.
5. Teléfono del investigador.
6. Firma del participante.
7. Firma del investigador principal.
8. Firmas de los testigos.

Como puede observarse los elementos eliminados en ambos formatos son prácticamente los mismos. El único elemento que no se encuentra en ambos formatos es el “Número de Proyecto”, elemento que sólo está presente en el Formato 2 de las cartas de consentimiento.

En relación con el **código numérico de identificación**, el Instituto Nacional de ciencias Médicas y Nutrición Salvador Zubirán argumentó que dicho código, en asociación con otros datos y elementos de información a los que se les ha asignado el mismo código, podría llevar a la identificación de la persona³²⁷. En consecuencia, el IFAI determinó que este elemento debía ser **omitido** en las versiones públicas que serían enviadas al recurrente.

En relación con el **nombre del investigador y su apellido** (ya que en ocasiones aparece solo el nombre o el apellido), **su teléfono, firma y nombre de la unidad en donde se realizó la investigación**, el Instituto Zubirán argumentó que muchas veces los esposos o familias de las participantes desconocen que éstas están esterilizadas, ya que algunas pacientes se reservan para su intimidad esa situación. En este sentido, efectivamente, dada la estrecha relación que muchas pacientes llegan a forjar a lo largo del proyecto con el investigador, según argumentó el citado Instituto, éste muchas veces es conocido por los esposos de las participantes o por otros de sus familiares. Por lo tanto, si el nombre del investigador o su teléfono fuera público podría permitir conocer, a los esposos o familiares que lo desconocen, que las participantes están esterilizadas o al menos presumir razonablemente esa situación. Y aquí la mera presunción podría colocar a la paciente en situación de riesgo, dada la naturaleza extremadamente sensible del asunto en cuestión. En relación con publicidad de la firma del investigador ocurriría de la misma manera, ya que aunque el nombre del investigador no apareciera en su firma, la Secretaría de Salud cuenta con un registro de firmas y rúbricas de los servidores públicos del sector salud que es público y por medio del cual podría averiguarse el nombre del investigador. Por lo tanto, el IFAI determinó que estos datos debían ser **omitidos** en las versiones públicas que serían enviadas al recurrente.

En relación con la **firma de la participante**, es importante señalar que este dato claramente constituye un dato personal que no puede ser revelado sin previa autorización de la titular del dato, ya que su divulgación afectaría directamente la intimidad de la persona, ya que de ésta se revelaría su identidad, ya sea porque en la firma se pueda leer el nombre de la participante o porque resulte conocida

³²⁷ Pues éste código fue usado, a decir del propio Instituto, en las muestras que fueron tomadas a cada paciente y en los apuntes del experimento.

para su esposo o familiares. En consecuencia, el IFAI determinó que este elemento debía ser **omitido** en las versiones públicas que serían enviadas al recurrente.

En lo que hace a la **firma de los testigos**, el Instituto Zubirán refiere que de conformidad con el artículo 22 fracción III del Reglamento de la Ley General de Salud, establece que en materia de investigación para la salud, los testigos deben tener alguna relación con el individuo sujeto a investigación. En este sentido, conocer la firma de los testigos permitiría hacer especulaciones o presunciones razonables sobre la identidad de cada una de las participantes. Por lo anterior, el IFAI determinó que este elemento debía ser **omitido** en las versiones públicas que serían enviadas al recurrente.

En cuanto al **número de proyecto**, dato que aparece únicamente en el formato 2 de las cartas de consentimiento, el Instituto Zubirán argumentó que es un dato que en asociación con otros permitiría conocer la identidad de las participantes. Sin embargo, en este elemento el Instituto Federal de Acceso a la Información Pública refirió que el número de proyecto es un número que sirve para que el Instituto Zubirán o la Secretaría de Salud identifiquen el proyecto y no se relaciona de manera alguna con las participantes. Por lo tanto, no se desprendía de qué manera podría identificarse a las participantes al conocerse el número del proyecto. Por lo anterior, resultaba evidente que para el número del proyecto no se actualiza ninguna de las causales de reserva establecidas en la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental, por lo que dicho dato no podrá ser excluido de las versiones públicas que sean entregadas al recurrente.

Por lo anterior el Instituto Federal de Acceso a la Información Pública procedió a **modificar la respuesta** del Instituto Nacional de Ciencias Médicas y Nutrición Salvador Zubirán, y le instruyó para que entregara al recurrente una versión pública de cada una de las 45 cartas de consentimiento en las que sólo debía omitirse los datos señalados en párrafos anteriores.

Resolución 187/2007, de 25 de abril

Número de expediente: 187/07. Recurrente: Silvia Carmen Otero López.
Ponente: Alonso Lujambio Irazábal. Dependencia ante la que se presentó la

solicitud: Procuraduría General de la República. Resolución de fecha: 25 de Abril de 2007.

En los considerandos de la resolución, se advierte del razonamiento del IFAI, que la **petición** de la recurrente con relación a Vicente Fox Quesada, es la siguiente: 1) El número (o cantidad) de *averiguaciones previas* que se integran actualmente en las que aparece como presunto responsable del algún delito. Al respecto se debe señalar que, en una solicitud, la recurrente planteó el presente contenido de información como si se tratara de dos contenidos diversos: (i) número de averiguaciones previas que se integran actualmente en contra de Vicente Fox; y (ii) en cuántas aparece como presunto responsable de algún delito. No obstante lo anterior, el Instituto interpreta que ambos contenidos se subsumen en el apuntado anteriormente, al tratarse de un mismo concepto; 2) Presuntos delitos cometidos (o como lo planteó la recurrente en su solicitud, “de qué ilícitos se trata”); 3) Números de expediente de dichas averiguaciones previas integradas actualmente; 4) Número (o cantidad) de casos en los que se decretó el no ejercicio de la acción penal en su contra; 5) Presuntos delitos cometidos en los casos en los que se determinó el no ejercicio de la acción penal y; 6) Números de expediente en los casos en los que se determinó el no ejercicio de la acción penal.

En su **respuesta**, la Procuraduría General de la República señaló a la recurrente que la información solicitada se encontraba clasificada como *reservada por un periodo de 12 años*, con fundamento en lo dispuesto por los artículos 13 fracción V, 14 fracción III, y 15 de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental.

Inconforme con la respuesta, la recurrente interpuso **recurso de revisión** ante el Instituto, en el que impugnaba la negativa de acceso a la información por parte de la autoridad por considerarla reservada. Reiteró así su solicitud original y además, señaló que lo solicitado constituía datos generales que no afectaban el curso de las pesquisas abiertas. Apuntando, además, que el argumento parecía más una forma de proteger la imagen del ex mandatario, cuando la Procuraduría General de la República está obligada a dar cuenta sobre su actuación, sobre todo al considerar que a lo largo del sexenio se presentaron varias denuncias en las que se implicaba al entonces titular del Ejecutivo; y que la dependencia federal debería

abrir al escrutinio este tipo de información, sin que esto implique que las indagatorias que aún están en curso pudieran verse afectadas.

En vía de **alegatos**, la Procuraduría General de la República precisó lo siguiente: 1) Que el caso versaba sobre información relativa a averiguaciones previas respecto de una persona determinada, por lo que se trataba de datos personales concernientes a una persona en particular, razón por la cual la información solicitada tenía el carácter de confidencial, en términos del artículo 18, fracción II de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental; 2) Que para poder difundir la información solicitada, se requería del consentimiento expreso del titular de la información confidencial, razón por la cual estaba justificada la negativa de acceso; 3) Que el artículo 16 del Código Federal de Procedimientos Penales establecía que sólo podían tener acceso a las actuaciones en la averiguación previa el inculpado, su defensor y la víctima u ofendido. Consecuentemente, para que un ciudadano tuviese acceso a la información relativa a las averiguaciones previas, debería acreditar el derecho que le asistía ante la autoridad competente; 4) Que el hecho de hacer público que existen averiguaciones previas en contra de cualquier persona, generaría desprestigio hacia el individuo de que se trate ya que vulnera el principio de presunción de inocencia y; 5) Que reiteraba la clasificación de la información solicitada con fundamento en los artículos 13 y 14 de la Ley de la materia.

En este sentido la presente resolución tendría por objeto *determinar la debida clasificación* de la información solicitada a la luz de los artículos 18, fracción II, 13, fracción V y 14, fracción III de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental. Además, es de mencionar, que la PGR no se pronunció específicamente sobre la existencia o inexistencia de averiguaciones previas, sino que se limitó a señalar que la información solicitada era confidencial, en los términos de los artículos señalados anteriormente.

Para **determinar la procedencia**, o no, **como confidencial de la información** relativa al nombre de una persona en relación con la existencia o inexistencia de averiguaciones previas en su contra, el Instituto determinó que el análisis se efectuaría **sin considerar el carácter de ex mandatario** de la persona señalada en la solicitud. El análisis, primeramente, determinaría si debe ser

confidencial la información relativa al nombre de cualquier persona asociado a la existencia o inexistencia de averiguaciones previas en relación con ella –en trámite o en las que se decretó el no ejercicio de la acción penal-, en razón de si la publicidad de dicha información revelaba datos personales que incidiesen en la intimidad de la misma. Y una vez determinado lo anterior, la presente resolución analizaría si existían **elementos de excepción aplicables** al caso concreto, considerando las características de la persona identificada en la solicitud.

En este sentido, los datos personales³²⁸ de una persona física que requieran del consentimiento de ésta para su difusión, al referirse a aspectos relativos a su intimidad, son protegidos por la Ley como información confidencial³²⁹. Cabe señalar que es claro que *dicha protección se extiende a cualquier persona física, sin hacer distinción de si la misma es o ha sido servidor público.*

Ahora bien, en el caso de la información relativa a las averiguaciones **previas en trámite** (en cuántas de éstas se señala como presunto responsable a una persona, los presuntos delitos cometidos y los números de expediente), esto es, investigaciones que aún no arrojan un resultado –consignación o no ejercicio de la acción penal-, *la publicidad de la información solicitada permitiría conocer la existencia de una investigación sobre cierta persona en relación con cierto presunto delito que no ha sido debidamente probado*, esto es, se permitiría conocer que una persona se encuentra sujeta a un procedimiento en el que no se han acreditado, ni siquiera a nivel administrativo, los elementos de convicción mínimos que permitan determinar si debe iniciarse o no un proceso penal ante autoridad judicial, y ello, en sí mismo, *puede incidir en la privacidad de dicha persona*, por lo que es ella quien debe decidir si desea que se dé a conocer que se encuentra sujeta a una investigación.

Por otra parte, la recurrente también solicitó acceso a información relacionada con **averiguaciones previas** en las que la PGR hubiere determinado el

³²⁸ El artículo 3, fracción II de la Ley de la materia, establece que se considerarán datos personales *la información concerniente a una persona física, identificada o identificable, entre otra*, la relativa a su origen étnico o racial, o que esté referida a las características físicas, morales o emocionales, a su vida afectiva y familiar, domicilio, número telefónico, patrimonio, ideología y opiniones políticas, creencias o convicciones religiosas o filosóficas, los estados de salud físicos o mentales, las preferencias sexuales, *u otras análogas que afecten su intimidad.*

³²⁹ El artículo 18, fracción II de la Ley señala que se considera *información confidencial*, la relativa a los datos personales que requieran el consentimiento de los individuos para su difusión, distribución o comercialización en los términos de dicha Ley.

no ejercicio de la acción penal en contra de la persona respectiva (específicamente solicitó conocer el número de casos en los que esto sucedió, de qué presuntos delitos se trató y los números de expediente correspondientes). En el caso de la información relativa a las averiguaciones previas en las que se determinó el *no ejercicio de la acción penal* por parte del Ministerio Público, subsiste la obligación de *proteger los datos personales* de los individuos que fueron sujetos a una investigación, toda vez que permitir que sea conocido el hecho de que una persona estuvo sujeta a una investigación en la cual se llegó a la conclusión de que no había delito que perseguir –por alguna de las causales que establecen las normas respectivas-, *incide en la intimidad de los individuos* que en su momento fueron investigados, por lo que deben ser estos quienes determinen si esa información debe o no ser del conocimiento público.

Ahora bien, cabe señalar que la recurrente relacionó **específicamente a una persona** respecto de los contenidos de información solicitados, esto es, un nombre en relación con el hecho de que se inició un procedimiento de investigación en su contra. En ese sentido, la publicidad de la información permitiría incidir negativamente en la privacidad de la persona respectiva, tanto en el caso de que la investigación se encuentre en trámite como en el caso de que la investigación por parte del Ministerio Público no haya reunido los elementos necesarios para acreditar el cuerpo del delito y la probable responsabilidad del indiciado, puesto que en ambos casos no existen –todavía, o en definitiva- elementos que permitan determinar que existe un delito, por lo que se trata de información que debe ser protegida. En otras palabras, en los casos en los cuales se requiere conocer si una persona estuvo o está sujeta a una averiguación previa, **no resulta procedente señalar siquiera si lo estuvo, está o no**, en virtud de que ello, en sí mismo, forma parte de la **privacidad** de la persona de que se trate, y será dicha persona quien, como titular de la información, determinará si la misma puede o no ser pública.

Llevando el presente argumento al extremo, de *hacer del conocimiento público la existencia de averiguaciones previas* (en el caso de aquellas que se encuentran en trámite) *en contra de determinado sujeto*, como es el caso en concreto, *podría desprestigiar al individuo de que se trate al revelar públicamente información* que posiblemente no constituya verdad jurídica alguna, creando

opiniones adversas a su persona, posiblemente de manera infundada³³⁰. Por lo tanto el Instituto determina que *la respuesta* de la Procuraduría General de la República en el **sentido de no afirmar ni negar la existencia** de una averiguación previa con las características apuntadas en la solicitud, resulta *procedente*.

Se considera, por lo tanto, que **la protección de la privacidad y de los datos personales constituye una garantía individual, un derecho humano internacionalmente reconocido**. Así mismo, el documento que estudiamos, destaca de forma importante que *dicha protección se extiende a cualquier persona, sin distinción*, por lo que los razonamientos vertidos en relación con la clasificación de la información relacionada con si una persona se encuentra sujeta o estuvo sujeta a una investigación de la que no se han derivado o no se derivaron en definitiva elementos de convicción en relación con la existencia de un delito, resultan aplicables a cualquier individuo que se ubique en dicha circunstancia, a menos que resulte aplicable una excepción debidamente fundada y motivada.

Existen objetivos de la Ley, que por excepción se pueden contraponer, como el de **transparentar la gestión pública** mediante la información que generen los sujetos obligados y favorecer la rendición de cuentas a los ciudadanos; y de garantizar la **protección de los datos personales** en posesión de los sujetos obligados. En este sentido, el Instituto aclara que **ambos objetivos son igualmente importantes y tienen la misma jerarquía normativa**, y su observancia, esto es, el cumplimiento de ambos, contribuye a la *democratización de la sociedad mexicana* y la plena vigencia del Estado de Derecho, en términos del artículo 4 de la Ley de

³³⁰ En este tenor, en razón del derecho a la protección de la privacidad que tiene toda persona, la información solicitada relacionada con la existencia de averiguaciones previas en trámite o en las que se determinó el no ejercicio de la acción penal, constituye información confidencial con fundamento en el artículo 18, fracción II de la Ley de la materia, en relación con el artículo 3, fracción II de la Ley en cita, puesto que la existencia o no de una averiguación previa en trámite o en la que se haya determinado el no ejercicio de la acción penal en contra de persona determinada, es información que sólo esa persona tiene derecho a conocer. Esta misma resolución, y en refuerzo a lo analizado, el IFAI señala que, al igual que la Constitución Política de los Estados Unidos Mexicanos –en su artículo 16- y la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental, los tratados internacionales firmados por México, y que constituyen, en concordancia con el artículo 133 constitucional, Ley Suprema de la Unión, establecen el derecho a la protección de la vida privada y de la honra y reputación de las personas. Para estos efectos, la citada resolución, refiere a la Declaración Universal de los Derechos Humanos de 1948 (artículo 12), Pacto Internacional de los Derechos Civiles y Políticos de 1966 y ratificado por México en 1981 (artículo 17) y Convención Americana sobre Derechos Humanos señala (artículo 11).

la materia³³¹. Y por lo tanto, armonizando ambos mandatos -y *a menos que, por excepción, uno se sobreponga al otro*- en principio podría confirmarse la clasificación de la información solicitada, toda vez que no resulta procedente afirmar o negar la existencia de averiguaciones previas en relación con una persona identificada³³².

Además, el IFAI, hace notar que el criterio relativo a que la información que implica identificar a una persona en relación con el hecho de que estuvo sujeta a una **averiguación previa** en la que se determinó el no *ejercicio de la acción penal*, es **confidencial**, ha sido adoptado con anterioridad por el mismo Instituto³³³. Asimismo, en diversas resoluciones determinó clasificar como **reservada** la información relativa a averiguaciones previas en trámite, incluyendo la identificación de la persona del investigado en relación con la existencia de la indagatoria³³⁴. Por otro lado, el Instituto recuerda la determinación hecha a que la sola **afirmación o negación de la existencia de cierta información en los archivos de una dependencia** o entidad **puede dar a conocer, en sí mismo, un dato personal**³³⁵, por lo cual, toda información relacionada con ello –siempre que no pueda desvincularse de la identificación de su titular-, como lo es en el presente caso, constituye información confidencial.

Por otro lado, refiere el Instituto que sin perjuicio de la procedencia de la clasificación analizada en los considerandos, es de señalar que pueden existir **excepciones a la mencionada confidencialidad**, por ejemplo, en el caso de *información que haya sido publicada de manera oficial por la Procuraduría General de la República o en otros medios*.

³³¹ Artículo 4. Son objetivos de esta Ley: I. Proveer lo necesario para que toda persona pueda tener acceso a la información mediante procedimientos sencillos y expeditos; II. Transparentar la gestión pública mediante la difusión de la información que generan los sujetos obligados; III. Garantizar la protección de los datos personales en posesión de los sujetos obligados; IV. Favorecer la rendición de cuentas a los ciudadanos, de manera que puedan valorar el desempeño de los sujetos obligados; V. Mejorar la organización, clasificación y manejo de los documentos, y VI. Contribuir a la democratización de la sociedad mexicana y la plena vigencia del Estado de derecho.

³³² Ello, con fundamento en el artículo 18 fracción II de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental, en relación con el artículo 3, fracción II de la misma.

³³³ En las resoluciones de los recursos de revisión números 1825/06 –presentado por el Comisionado Alonso Gómez Robledo Verduzco-, 2288/06 –presentado por la Comisionada María Marván Laborde- y 325/07 –presentado por el Comisionado Ponente del recurso de revisión que se estudia.

³³⁴ Es el caso de la resolución del recurso de revisión número 2326/06 –presentado por el Comisionado Alonso Gómez Robledo Verduzco.

³³⁵ Caso de la resolución del recurso de revisión número 891/05 presentado por la Comisionada María Marván Laborde, interpuesto en contra del Instituto Nacional de Migración, así lo refiere la resolución que estudiamos.

Asimismo, es de señalar que **los anteriores razonamientos se emiten en relación con aquellas averiguaciones previas que se encuentran en trámite y en las que se determinó el no ejercicio de la acción penal.** Cuestión distinta es aquella que se refiere a los procesos penales –ante el Poder Judicial- en los cuales se tienen elementos de convicción respecto de la existencia de un delito, por lo que las normas aplicables establecen la publicidad de ciertos datos relativos a dichos procesos. En ese sentido, si bien la *información confidencial no se encuentra sujeta a plazos de vencimiento, la misma puede perder ese carácter*, entre otros, en virtud de una **excepción** establecida en ley, **como es el caso de ciertos datos que se hacen públicos al momento en que una averiguación previa es consignada ante los tribunales.** Lo anterior, a partir de las normas aplicables al proceso penal, que señalan la publicidad del mismo.

Ahora bien, cabe destacar que la PGR también clasificó los contenidos de información solicitada como **reservados** con fundamento en los artículos 13, fracción V y 14, fracción III de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental. El artículo 13 refiere que, como información reservada podrá clasificarse aquella cuya difusión pueda: (...) V. Causar un serio perjuicio a las actividades de verificación del cumplimiento de las leyes, prevención o persecución de los delitos, la impartición de la justicia, la recaudación de las contribuciones, las operaciones de control migratorio, las estrategias procesales en procesos judiciales o administrativos mientras las resoluciones no causen estado. Ahora bien, por su parte, el artículo 27 del Reglamento de la Ley Federal de Transparencia y Acceso a la Información Pública gubernamental – Reglamento de la Ley- dispone que los titulares de las unidades administrativas, al clasificar expedientes y documentos como reservados, deberán tomar en consideración el daño que causaría su difusión a los intereses tutelados, entre otros, en el artículo 13 de la Ley. Así mismo, la resolución refiere los numerales 8, 24 y 26 de los Lineamientos generales para la clasificación y desclasificación de información de las dependencias y entidades de la Administración Pública Federal. En consecuencia, el Instituto refiere que es posible concluir que **es procedente la clasificación** respecto de la información relativa a una persona determinada (o al nombre de una persona, quien quiera que sea) asociado con la existencia o inexistencia de averiguaciones previas en relación con ella, y por lo tanto el IFAI

determinó que dicha información es confidencial, por revelar datos personales que inciden en la intimidad de las personas.

Ahora bien, y atendiendo a las características particulares del caso, cabe señalar que tanto el derecho de **acceso a la información pública** como el derecho a la **protección de datos personales** admiten ciertos **límites**, expresados en disposiciones legales que contienen las causales específicas que impiden su difusión en el caso del primero, o que permiten su apertura en el caso del segundo. En este sentido, tratándose de información contenida en los archivos de las dependencias y entidades, su acceso puede verse limitado por razones de Estado (**reserva**) o bien, por tratarse de información de los particulares (**confidencialidad**). Respecto de los datos referidos a una persona, obtenidos por las entidades públicas en ejercicio de sus atribuciones, las limitaciones en el acceso encuentran su principal justificación en los derechos de tercero, particularmente en la protección de la esfera de intimidad y el patrimonio de las personas (particulares). En otras palabras, la *confidencialidad de la información está destinada a proteger la esfera de acción de los particulares respecto de la injerencia indebida de la autoridad y de otros particulares.*

Ahora bien, dicha excepción viene a colación, en virtud de que la persona respecto de la cual se solicita información en este caso, es ex Presidente de México, esto es, la persona respectiva fue titular de uno de los tres Poderes de la Unión –el único de carácter unipersonal- de los años 200 a 2006, y constituye, por tanto, una persona de gran trascendencia en el contexto socio-político, no sólo histórico, sino actual de México. Por lo anterior, el Instituto consideró procedente **ponderar la protección de la privacidad** analizada en párrafos anteriores, **frente al interés de la sociedad en general de conocer la información** solicitada³³⁶. En ese sentido, pueden existir situaciones en las cuales el interés social de conocer deba prevalecer sobre el interés de proteger información de un individuo, es decir, **situaciones en las que el bien que se busca obtener con la apertura de cierta información es superior al daño que se causaría al o los particulares al vulnerar su derecho a**

³³⁶ Se presenta una clara tensión entre la necesidad de proteger cierta información que se refiere a la privacidad de una persona, y el interés de la sociedad en general de conocerla. Se está en presencia del interés de la sociedad por conocer la información relativa a la persona de un ex Presidente de la República Mexicana. Es en estos casos en los cuales se realiza el juicio ponderativo de acuerdo a la ley para determinar si resulta válida la limitación al derecho al honor y a la privacidad.

la privacidad. El IFAI reconocía que existía, por un lado, la obligación de proteger la privacidad de cualquier persona, y por el otro, el interés de la sociedad de conocer la existencia de investigaciones relativas a personajes de la vida pública, como era la situación. Ello permitía concluir que en el caso concreto, como situación excepcional, procede la divulgación de ciertos datos personales. Esta determinación encuentra su fundamento de manera estricta en los objetivos que persigue la Ley, en las características de la persona respecto de quien se solicita información y en el **principio de máxima publicidad** consignado en el artículo 6 de la propia Ley³³⁷.

Por tanto, a partir del principio de máxima publicidad³³⁸, el Instituto determinó **procedente otorgar acceso a la información** solicitada, considerando que a partir de la misma, *los ciudadanos que han sido gobernados por la persona mencionada en la solicitud, puedan contar con mayores elementos para valorar la gestión pública que en su momento llevó a cabo dicha persona, así como su desempeño y en última instancia, tomar decisiones mejor informadas*, con lo cual **se favorece la rendición de cuentas por parte de los servidores públicos, se contribuye a la democratización de la sociedad mexicana** y a la plena vigencia del Estado de Derecho. Y bien, *si en principio, la información sí actualiza una causal de clasificación, en el caso que nos ocupa, por las circunstancias especiales del caso, se exceptúa su aplicación, en virtud de que el Instituto advertía el interés mayor de conocer la misma, el cual se sobrepone a la posible afectación de la intimidad del individuo.*

El interés de la sociedad en conocer de la información solicitada, así como las circunstancias especiales del caso, razonó el Instituto, se corroboran con los diversos boletines y publicaciones que se reproducen en el sexto considerando de la resolución, de los que podía advertirse que los asuntos respectivos han sido

³³⁷ Artículo 6. En la interpretación de esta Ley y de su Reglamento, así como de las normas de carácter general a las que se refiere el Artículo 61, se deberá favorecer el principio de máxima publicidad y disponibilidad de la información en posesión de los sujetos obligados.

El derecho de acceso a la información pública se interpretará conforme a la Constitución Política de los Estados Unidos Mexicanos; la Declaración Universal de los Derechos Humanos; el Pacto Internacional de Derechos Civiles y Políticos; la Convención Americana sobre Derechos Humanos; la Convención Sobre la Eliminación de Todas las Formas de Discriminación Contra la Mujer, y demás instrumentos internacionales suscritos y ratificados por el Estado Mexicano y la interpretación que de los mismos hayan realizado los órganos internacionales especializados.

³³⁸ Establecido en el artículo 6, en concordancia con los objetivos en el artículo 4 de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental.

públicamente ventilados por la PGR y por medios de comunicación, en razón del interés que tienen para la sociedad y de los temas que abordan las investigaciones de que se trata, en relación con la persona de quien en su momento fue Presidente de México. En consecuencia, resultaba procedente instruir a la Procuraduría para que entregase a la recurrente la información específicamente solicitada, en relación con averiguaciones previas en trámite y en las que se decretó el no ejercicio de la acción penal³³⁹.

De los razonamientos anteriores es como el Instituto concluyó **revocar la respuesta** otorgada por la PGR.

Resolución 487/2007, de 25 de abril

Número de expediente: 487/07. Recurrente: Idalia Gómez. Ponente: Alonso Lujambio Irazábal. Dependencia ante la que se presentó la solicitud: Procuraduría General de la República. Resolución de fecha: 25 de Abril de 2007.

En los considerandos de la resolución el IFAI desglosa en dos partes la **petición** de la recurrente, de la siguiente forma: 1) Cantidad de *averiguaciones previas* en las que aparece Jorge Hank Rhon como presunto responsable, números de expediente y delitos que se le imputan en cada uno y; 2) Cantidad de *procesos penales* en los que aparece Jorge Hank Rhon como *presunto responsable*, números de expediente y delitos que se le imputan en cada uno. Además de las manifestaciones para ambos requerimientos con relación a que la información solicitada se hiciera respecto de los expedientes en trámite, archivados, en reserva o ejecutoriados. Así mismo señaló que debía buscarse en las tres Subprocuradurías del sujeto obligado.

En su **respuesta**, la Procuraduría General de la República señaló a la recurrente que la información solicitada se encontraba clasificada como *reservada*

³³⁹ Cabe señalar que de acuerdo a lo que se señala en relación con lo difundido por de medios de comunicación, el Instituto tenía evidencia de que existían averiguaciones previas en las que se había decretado el no ejercicio de la acción penal en relación con Vicente Fox Quesada. Sin embargo, considerando que las notas periodísticas citadas en la resolución se referían a la presentación de denuncias en relación con dicha persona, pero no así a la existencia de averiguaciones previas en trámite. Por lo que, en caso de que a la fecha de cumplimiento de la presente resolución, la PGR no contaba con averiguaciones previas en trámite en relación con Vicente Fox Quesada, debería declarar la inexistencia de dicha información en términos de los artículos 46 de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental y 70 fracción V de su Reglamento.

por un periodo de 12 años, con fundamento en lo dispuesto por los artículos 13 fracción V y 14 fracciones I y III de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental. A mayor abundamiento, el sujeto obligado señaló lo siguiente en su respuesta: 1. Que se había consultado a las tres Subprocuradurías competentes para conocer de la información solicitada, de conformidad con la Ley Orgánica de la Procuraduría General de la República: (i) de Investigación Especializada en Delitos Federales; (ii) de Control Regional, Procedimientos Penales y Amparo; y (iii) de Investigación Especializada en Delincuencia Organizada. 2. Que se había negado la información por tratarse de información clasificada como reservada con fundamento en los artículos 13 fracción V y 14 fracciones I y III, de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental. 3. Que atento al criterio emitido por el Comité de Información de la Procuraduría General de la República, en el sentido de clasificar como reservada la información relacionada con averiguaciones previas en trámite, no era posible otorgar la información solicitada³⁴⁰. 4. Que además, la Subprocuraduría de Investigación Especializada en Delincuencia Organizada manifestó, en relación a los procesos penales, que la información solicitada pudiera estar en el Poder Judicial de la Federación, toda vez que le compete el conocimiento de los procesos penales, y por lo tanto se sugirió al hoy recurrente dirigir su petición a la unidad de enlace del Consejo de la Judicatura Federal.

Inconforme con la respuesta, la recurrente interpuso **recurso de revisión** ante el Instituto, manifestando que: 1) La respuesta del sujeto era incompleta; 2) La respuesta proporcionada era ambigua porque determinaba la reserva de la información sin especificar por cuánto tiempo lo sería; 3) La reserva de la información solicitada evadía el espíritu de la ley e impedía conocer la eficacia y eficiencia del trabajo del sujeto obligado; 4) Era posible que varias de las averiguaciones previas o expedientes tuviesen muchos años en trámite y era público que existían expedientes que ya habían causado estado; 5) Los expedientes que ya causaron estado podían ser consultados protegiendo la información

³⁴⁰ Dicho criterio fue emitido por el Comité de Información de la Procuraduría en su Décimo Cuarta Sesión Ordinaria de Trabajo 2005, conforme a lo dispuesto por el artículo 14 fracción III de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental, en relación con el Vigésimo Sexto de los Lineamientos Generales para la clasificación y desclasificación de la información de las dependencias y entidades de la Administración Pública Federal, y lo dispuesto por el artículo 16 del Código Federal de Procedimientos Penales.

confidencial y; 6) Se debía considerar que el argumento de que el indiciado puede evadirse de la acción de la justicia o que se entorpezca una indagatoria, no podía ser admitido, pues la Constitución Política de los Estados Unidos Mexicanos prevé que toda persona tiene derecho a defenderse y el Ministerio Público está obligado a citarlo a comparecer e incluso a aceptar las pruebas que presente para su defensa, y que por lo tanto, no sería a través de una solicitud de acceso como el indiciado se enterara de los expedientes abiertos en su contra y mucho menos, considerando la generalidad de los planteamientos de la solicitud de acceso.

En vía de **alegatos**, la Procuraduría General de la República precisó lo siguiente: 1) Que con motivo de la solicitud de acceso presentada por la recurrente, la Unidad de Enlace dirigió oficios a las Subprocuradurías de: (i) Control Regional, Procedimientos Penales y Amparo; (ii) de Investigación Especializada en Delitos Federales; y (iii) de Investigación Especializada en Delincuencia Organizada, por estar en el ámbito de su competencia, además de que la recurrente las señaló como dato para la localización de la información; 2) Que en respuesta a dicha solicitud, la Subprocuraduría de Investigación Especializada en Delincuencia Organizada dio respuesta reservando la información toda vez que la petición no se encuadra en los supuestos de inculpado, víctima u ofendido que exige el artículo 20 Constitucional, considerando que las indagatorias que integra el Ministerio Público de la Federación contienen información a la cual no puede tener acceso cualquier persona, sólo las partes en tales asuntos; 3) Que la Subprocuraduría de Investigación Especializada en Delitos Federales reportó que en la Unidad Especializada en Delitos Cometidos por Servidores Públicos se localizó registro de *una averiguación previa*; 4) Que la Subprocuraduría de Control Regional, Procedimientos Penales y Amparo informó haber encontrado la *averiguación previa 4303/D/95*, misma que fue consignada en el Juzgado 9° con sede en el Reclusorio Preventivo Sur; 5) Que no obstante los informes remitidos por las Subprocuradurías mencionados, se notificó al peticionario la reserva de la información solicitada en virtud del criterio emitido en la décima cuarta sesión ordinaria de trabajo de la Procuraduría General de la República; 6) *Reiteró la clasificación* de la información solicitada como *reservada* con fundamento en lo dispuesto por los artículos 13 facción V y 14 fracciones I y III de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental, en relación con

el artículo 16 del Código Federal de Procedimientos Penales y el artículo 225 del Código Penal Federal; 7) Que por lo que se refiere al plazo de la reserva, la Ley de Transparencia, en su artículo 15 señala que la información clasificada como reservada con fundamento en los artículos 13 y 14 de la Ley, podrá permanecer con ese carácter hasta por un período de 12 años y que la temporalidad de las indagatorias y sus investigaciones es atribución del ministerio público; 8) Que respecto a los argumentos de la hoy recurrente respecto a que el argumento de reserva evade el espíritu de la ley al no permitir a los ciudadanos acceder a la información, es de advertir que si bien el espíritu de la Ley de Transparencia es permitir a los ciudadanos acceder a la información pública, también lo es que la propia ley contiene preceptos para la *protección de datos personales* de los individuos; 9) Que la Subprocuraduría de Investigación Especializada en Delincuencia Organizada indicó que, en el caso que nos ocupa, la solicitud está íntimamente relacionada con datos personales del involucrado en alguna indagatoria, por lo que el simple hecho de mencionar un número cualquiera que sea, ya se estaría afectando la intimidad del individuo, sin importar que dicha persona sea un personaje público de gran relevancia, pues la ley no hace distinciones al efecto, por lo que se reitera que los datos personales cuentan con protección especial de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental, clasificándola como información confidencial, atento a lo dispuesto por la fracción II del artículo 18 de la Ley. Por lo tanto, los *datos personales* están protegidos por los artículos 3, fracción II, 18 fracción II y 19, así como el capítulo IV de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental y; 10) Por otra parte, por lo que se refiere al señalamiento del recurrente respecto a que existen expedientes que ya causaron estado y pueden ser consultados adoptando las medidas necesarias para proteger la *información confidencial*, es de resaltar que si se trata de cosa juzgada es competencia de la administración de justicia, por lo que en relación a los procesos penales se reitera la sugerencia de que se solicite dicha información al Poder Judicial de la Federación.

En **alcance a sus alegatos**, la Procuraduría General de la República manifestó lo siguiente: 1) Que la Subprocuraduría de Investigación Especializada en Delitos Federales se declaró incompetente en la averiguación previa número 4303/D/95 (misma que se abrió por triplicado, como lo había señalado la

Subprocuraduría de Control Regional, Procedimientos Penales y Amparo) remitiéndola a la Delegación del Distrito Federal, que acumuló todas; 2) Que dicha averiguación previa se consignó ante el Juez Noveno de Distrito de Procesos Penales Federales, quien el 30 de enero de 1998 *dictó sentencia absolutoria*, misma que se impugnó a través del recurso de apelación, la cual fue *confirmada* el 3 de septiembre del mismo año por el Segundo Tribunal Unitario del Primer Circuito, *bajo el toca 70/98* y; 3) Que la Subprocuraduría de Investigación Especializada en Delincuencia Organizada manifestó que se realizó una nueva búsqueda minuciosa en los expedientes reservados, libros de gobierno, archivos de trámite y archivos de concentración de las Unidades adscritas a dicha Subprocuraduría, *no encontrándose antecedente* alguno en relación con la información solicitada.

Posteriormente, y en los **considerandos** se establece que el **objetivo de la resolución** del IFAI es presentar el marco normativo aplicable a las averiguaciones previas; así como analizar la respuesta de la Procuraduría General de la República en relación con las *averiguaciones previas* que integra el Ministerio Público respecto de una persona, y lo relativo a los *procesos penales*, como es el caso de la averiguación previa número 4303/D/95, que concluyó en el Toca de apelación número 70/98.

Así el IFAI consideró en la presente resolución que el análisis debía efectuarse considerando si procedía la clasificación como confidencial de la información relativa al nombre de una persona en relación con la existencia o inexistencia de averiguaciones previas en su contra. Dicho estudio se haría independientemente del carácter de figura pública de la persona, y en razón de si la publicidad de dicha información revelaba datos personales que incidían en la intimidad del individuo; además de analizar si existían elementos de excepción aplicables al caso concreto.

El Instituto destacó que el artículo 3, fracción II de la Ley, establece que se considerarán **datos personales** *la información concerniente a una persona física, identificada o identificable, entre otra, la relativa a su origen étnico o racial, o que esté referida a las características físicas, morales o emocionales, a su vida afectiva y familiar, domicilio, número telefónico, patrimonio, ideología y opiniones políticas, creencias o convicciones religiosas o filosóficas, los estados de salud*

físicos o mentales, las preferencias sexuales, u otras análogas que afecten su intimidad. Y que, por su parte, el artículo 18, fracción II de la Ley señala que se considera **información confidencial**, la relativa a los *datos personales que requieran el consentimiento de los individuos para su difusión, distribución o comercialización* en los términos de dicha Ley. Por lo que, en este sentido, los datos personales de una persona física, de los referidos en el artículo 3 fracción II antes citado, que requieran del consentimiento de su titular para su difusión, al referirse a aspectos relativos a su intimidad, son protegidos por la Ley como información confidencial. Asentando que es claro que dicha protección se extendía a cualquier persona física, sin hacer distinción de si la misma es o ha sido servidor público.

Refiere la resolución que, cabe apuntar que en el caso de la información relativa a las averiguaciones previas en trámite (cuántas hay en las que se señala como presunto responsable a cierta persona, los presuntos delitos cometidos y los números de expediente), esto es, investigaciones que aún no arrojan un resultado –consignación o no ejercicio de la acción penal-, *la información solicitada permitiría relacionar el hecho de la existencia de una investigación sobre cierta persona relativa a cierto presunto delito que no ha sido debidamente probado*, esto es, se permitiría conocer que una persona se encuentra sujeta a un procedimiento en el que no se han acreditado, ni siquiera a nivel administrativo, los elementos de convicción mínimos que permitan determinar si debe iniciarse o no un proceso penal ante autoridad judicial, y ello, en sí mismo, *puede incidir en la **privacidad** de dicha persona, por lo que es ella quien debe decidir si desea que se dé a conocer que se encuentra sujeta a una investigación.*

Por otra parte, nos dice el Instituto, en los casos en que la Procuraduría General de la República hubiere determinado el *no ejercicio de la acción penal* en contra de la persona señalada en la solicitud de acceso, subsiste la *obligación de proteger los **datos personales*** de los individuos que fueron sujetos a una investigación, toda vez que permitir que sea conocido el hecho de que una persona estuvo sujeta a una investigación en la cual se llegó a la conclusión de que no había delito que perseguir –por alguna de las causales que establecen las normas respectivas-, *incide en la **intimidad** de los individuos que en su momento fueron*

investigados, por lo que deben ser estos quienes determinen si esa información debe o no ser del conocimiento público.

En el caso concreto, reflexiona el Instituto, la recurrente relacionó específicamente a una persona respecto de los contenidos de información solicitados, esto es, un nombre en relación con el hecho de que se inició un procedimiento de investigación en su contra. En ese sentido, *la publicidad de la información permitiría incidir negativamente en la **privacidad** de la persona respectiva*, tanto en el caso de que la investigación se encuentre en trámite como en el caso de que la investigación por parte del Ministerio Público no haya reunido los elementos necesarios para acreditar el cuerpo del delito y la probable responsabilidad del indiciado, puesto que en ambos casos no existen –todavía, o en definitiva- elementos que permitan determinar que existe un delito, por lo que se trata de información que debe ser protegida.

En otras palabras, *en los casos en los cuales se requiere conocer si una persona estuvo o está sujeta a una averiguación previa, no resulta procedente señalar siquiera si lo estuvo, está o no, en virtud de que ello, en sí mismo, forma parte de la privacidad de la persona de que se trate, y será dicha persona quien, como titular de la información, determinará si la misma puede o no ser pública. Ya que en el supuesto, de hacer del conocimiento público la existencia de averiguaciones previas (en el caso de aquellas que se encuentran en trámite) en contra de determinado sujeto –como es el presente caso- podría desprestigiar al individuo de que se trate al revelar públicamente información que posiblemente no constituya verdad jurídica alguna, creando opiniones adversas a su persona, posiblemente de manera infundada. En este tenor, en razón del derecho a la **protección de la privacidad** que tiene toda persona, la información solicitada relacionada con la existencia de *averiguaciones previas en trámite o en las que se determinó el no ejercicio de la acción penal, constituye información confidencial*³⁴¹.*

³⁴¹ El fundamento se encuentra en el artículo 18, fracción II de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental. Por lo tanto, la existencia o no de una averiguación previa en trámite o en la que se haya determinado el no ejercicio de la acción penal en contra de persona determinada, es información que sólo esa persona tiene derecho a conocer. Esta misma resolución, y en refuerzo a lo analizado, el IFAI señala que, al igual que la Constitución Política de los Estados Unidos Mexicanos –en su artículo 16- y la Ley Federal de Transparencia y

Se considera, por lo tanto, que **la protección de la privacidad y de los datos personales constituye una garantía individual, un derecho humano internacionalmente reconocido**. Así mismo, el documento que estudiamos, destaca de forma importante que *dicha protección se extiende a cualquier persona, sin distinción*, por lo que los razonamientos vertidos en relación con la clasificación de la información relacionada con si una persona se encuentra sujeta o estuvo sujeta a una investigación de la que no se han derivado o no se derivaron en definitiva elementos de convicción en relación con la existencia de un delito, resultan aplicables a cualquier individuo que se ubique en dicha circunstancia, a menos que resulte aplicable una excepción debidamente fundada y motivada.

Existen objetivos de la Ley, que por excepción se pueden contraponer, como el de **transparentar la gestión pública** mediante la información que generen los sujetos obligados y favorecer la rendición de cuentas a los ciudadanos; y de garantizar la **protección de los datos personales** en posesión de los sujetos obligados. En este sentido, el Instituto aclara que **ambos objetivos son igualmente importantes y tienen la misma jerarquía normativa**, y su observancia, esto es, el cumplimiento de ambos, contribuye a la *democratización de la sociedad mexicana* y la plena vigencia del Estado de Derecho, en términos del artículo 4 de la Ley de la materia³⁴². Y por lo tanto, armonizando ambos mandatos *-y a menos que, por excepción, uno se sobreponga al otro-* en principio podría confirmarse la clasificación de la información solicitada, toda vez que no resulta procedente afirmar o negar la existencia de averiguaciones previas en relación con una persona identificada³⁴³.

Acceso a la Información Pública Gubernamental, los tratados internacionales firmados por México, y que constituyen, en concordancia con el artículo 133 constitucional, Ley Suprema de la Unión, establecen el derecho a la protección de la vida privada y de la honra y reputación de las personas. Para estos efectos, la citada resolución, refiere a la Declaración Universal de los Derechos Humanos de 1948 (artículo 12), Pacto Internacional de los Derechos Civiles y Políticos de 1966 y ratificado por México en 1981 (artículo 17) y Convención Americana sobre Derechos Humanos señala (artículo 11).

³⁴² Artículo 4. Son objetivos de esta Ley: I. Proveer lo necesario para que toda persona pueda tener acceso a la información mediante procedimientos sencillos y expeditos; II. Transparentar la gestión pública mediante la difusión de la información que generan los sujetos obligados; III. Garantizar la protección de los datos personales en posesión de los sujetos obligados; IV. Favorecer la rendición de cuentas a los ciudadanos, de manera que puedan valorar el desempeño de los sujetos obligados; V. Mejorar la organización, clasificación y manejo de los documentos, y VI. Contribuir a la democratización de la sociedad mexicana y la plena vigencia del Estado de derecho.

³⁴³ Ello, con fundamento en el artículo 18 fracción II de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental, en relación con el artículo 3, fracción II de la misma.

Además, el IFAI, hace notar que el criterio relativo a que la información que implica identificar a una persona en relación con el hecho de que estuvo sujeta a una **averiguación previa** en la que se determinó el no *ejercicio de la acción penal*, es **confidencial**, ha sido adoptado con anterioridad por el mismo Instituto³⁴⁴. Asimismo, en diversas resoluciones determinó clasificar como **reservada** la información relativa a averiguaciones previas en trámite, incluyendo la identificación de la persona del investigado en relación con la existencia de la indagatoria³⁴⁵. Por otro lado, el Instituto recuerda la determinación hecha a que la sola **afirmación o negación de la existencia de cierta información en los archivos de una dependencia** o entidad **puede dar a conocer**, en sí mismo, un **dato personal**³⁴⁶.

Por otro lado, refiere el Instituto que sin perjuicio de la procedencia de la clasificación analizada en los considerandos –específicamente el cuarto-, es de señalar que pueden existir **excepciones a la mencionada confidencialidad**, por ejemplo, en el caso de *información* que haya sido *publicada de manera oficial por la Procuraduría General de la República o en otros medios*.

Asimismo, es de señalar que **los anteriores razonamientos se emiten en relación con aquellas averiguaciones previas que se encuentran en trámite y en las que se determinó el no ejercicio de la acción penal**. Cuestión distinta es aquella que se refiere a los procesos penales –ante el Poder Judicial- en los cuales se tienen elementos de convicción respecto de la existencia de un delito, por lo que las normas aplicables establecen la publicidad de ciertos datos relativos a dichos procesos. En ese sentido, si bien la *información confidencial no se encuentra sujeta a plazos de vencimiento, la misma puede perder ese carácter*, entre otros, en virtud de una **excepción** establecida en ley, **como es el caso de ciertos datos que se hacen públicos al momento en que una averiguación previa es consignada ante los tribunales**. Lo anterior, a partir de las normas aplicables al proceso penal, que señalan la publicidad del mismo.

³⁴⁴ En las resoluciones de los recursos de revisión números 1825/06 –presentado por el Comisionado Alonso Gómez Robledo Verduzco-, 2288/06 –presentado por la Comisionada María Marván Laborde- y 325/07 –presentado por el Comisionado Ponente del recurso de revisión que se estudia.

³⁴⁵ Es el caso de la resolución del recurso de revisión número 2326/06 –presentado por el Comisionado Alonso Gómez Robledo Verduzco.

³⁴⁶ Caso de la resolución del recurso de revisión número 891/05 presentado por la Comisionada María Marván Laborde, interpuesto en contra del Instituto Nacional de Migración, así lo refiere la resolución que estudiamos.

Se señala además que tanto el derecho de **acceso a la información pública** como el derecho a la **protección de datos personales** admiten ciertos **límites**, expresados en disposiciones legales que contienen las causales específicas que impiden su difusión en el caso del primero, o que permiten su apertura en el caso del segundo. En este sentido, tratándose de información contenida en los archivos de las dependencias y entidades, su acceso puede verse limitado por razones de Estado (**reserva**) o bien, por tratarse de información de los particulares (**confidencialidad**). Respecto de los datos referidos a una persona, obtenidos por las entidades públicas en ejercicio de sus atribuciones, las limitaciones en el acceso encuentran su principal justificación en los derechos de tercero, particularmente en la protección de la esfera de intimidad y el patrimonio de las personas (particulares). En otras palabras, *la confidencialidad de la información está destinada a proteger la esfera de acción de los particulares respecto de la injerencia indebida de la autoridad y de otros particulares.*

Ahora bien, dicha excepción viene a colación, en virtud de que la persona respecto de la cual se solicita información en este caso, es ex Presidente Municipal de Tijuana, Baja California y candidato entonces a gobernador de dicho estado. Por lo que ha sido y en ese momento era una persona de gran trascendencia en el contexto sociopolítico local y nacional del país. Por lo anterior, el Instituto consideró procedente **ponderar la protección de la privacidad** analizada en párrafos anteriores, **frente al interés de la sociedad en general de conocer la información** solicitada³⁴⁷. En ese sentido, pueden existir situaciones en las cuales el interés social de conocer deba prevalecer sobre el interés de proteger información de un individuo, es decir, **situaciones en las que el bien que se busca obtener con la apertura de cierta información es superior al daño que se causaría al o los particulares al vulnerar su derecho a la privacidad**. El IFAI reconocía que existía, por un lado, la obligación de proteger la privacidad de cualquier persona, y por el otro, el interés de la sociedad de conocer la existencia de investigaciones relativas a personajes de la vida pública, como era la situación. Ello permitía concluir que en el caso concreto, como situación excepcional,

³⁴⁷ Se presenta una clara tensión entre la necesidad de proteger cierta información que se refiere a la privacidad de una persona, y el interés de la sociedad en general de conocerla. Se está en presencia del interés de la sociedad por conocer la información relativa a la persona de un candidato a gobernador. Es en estos casos en los cuales se realiza el juicio ponderativo de acuerdo a la ley para determinar si resulta válida la limitación al derecho al honor y a la privacidad.

procede la divulgación de ciertos datos personales. Esta determinación encuentra su fundamento de manera estricta en los objetivos que persigue la Ley, en las características de la persona respecto de quien se solicita información y en el **principio de máxima publicidad** consignado en el artículo 6 de la propia Ley³⁴⁸.

Por tanto, a partir del principio de máxima publicidad³⁴⁹, el Instituto determinó procedente otorgar acceso a la información solicitada, considerando que a partir de la misma, *los ciudadanos que han sido gobernados por la persona mencionada en la solicitud, puedan contar con mayores elementos para valorar la gestión pública que en su momento llevó a cabo dicha persona, así como su desempeño y en última instancia, tomar decisiones mejor informadas, considerando que dicha persona actualmente busca ocupar un cargo de elección popular*, con lo cual se favorece la **rendición de cuentas** por parte de los servidores públicos, se contribuye a la democratización de la sociedad mexicana y a la plena vigencia del Estado de Derecho. Y bien, si en principio, la información sí actualiza una causal de clasificación, en el caso que nos ocupa, por las circunstancias especiales del caso, se exceptúa su aplicación, en virtud de que el Instituto advertía el interés mayor de conocer la misma, el cual se sobrepone a la posible afectación de la intimidad del individuo.

Por último, y en cuanto a la información solicitada a la PGR con relación a los procesos penales, es cierto como lo refiere la Institución que no es competencia de ella. Sin embargo, y por otro lado, es de señalar que cuando se decreta el ejercicio de la acción penal, la etapa de investigación que realiza el Ministerio Público concluyó, y por lo tanto, existen elementos suficientes para suponer que el inculpado pudo haber cometido un delito. Por lo que una vez decretado dicho ejercicio de la acción penal, la naturaleza de la información cambia, en virtud de que al haber consignado la averiguación previa ante los tribunales competentes ya

³⁴⁸ Artículo 6. En la interpretación de esta Ley y de su Reglamento, así como de las normas de carácter general a las que se refiere el Artículo 61, se deberá favorecer el principio de máxima publicidad y disponibilidad de la información en posesión de los sujetos obligados.

El derecho de acceso a la información pública se interpretará conforme a la Constitución Política de los Estados Unidos Mexicanos; la Declaración Universal de los Derechos Humanos; el Pacto Internacional de Derechos Civiles y Políticos; la Convención Americana sobre Derechos Humanos; la Convención Sobre la Eliminación de Todas las Formas de Discriminación Contra la Mujer, y demás instrumentos internacionales suscritos y ratificados por el Estado Mexicano y la interpretación que de los mismos hayan realizado los órganos internacionales especializados.

³⁴⁹ Establecido en el artículo 6, en concordancia con los objetivos en el artículo 4 de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental.

no existe razón para clasificar el nombre de la persona respecto de la cual ya no se están llevando a cabo facultades de investigación por parte del MP. Lo anterior considerando que el Poder Judicial de la Federación hace pública cierta información sobre los procedimientos en trámite³⁵⁰.

De los razonamientos anteriores es como el Instituto concluyó **modificar la respuesta** de la Procuraduría General de la República, a fin de que entregue a la recurrente la información específicamente solicitada, en relación con las averiguaciones previas en las que apareciere como presunto responsable Jorge Hank Rhon. En el caso de que aquella no contare con averiguaciones en las que apareciere éste como presunto responsable, debería de declarar la inexistencia de dicha información. Además de entregar a la recurrente la información que la PGR remitió al instituto en la sustanciación del recurso, así como el delito o delitos por los que se siguió la averiguación previa número 4303/D/95³⁵¹.

³⁵⁰ Tal es el caso que la Constitución en su artículo 20 fracción III, establece como garantía del inculpado que se le hará saber en audiencia pública, y dentro de las cuarenta y ocho horas siguientes a su consignación a la justicia, el nombre de su acusador y la naturaleza y causa de la acusación, a fin de que conozca bien el hecho punible que se le atribuye y pueda contestar el cargo, rindiendo en este acto su declaración preparatoria.

³⁵¹ Misma que fue consignada al Juez Noveno de Distrito de Procesos Penales Federales, quien el 30 de enero de 1998 dictó sentencia absolutoria, misma que se impugnó a través del recurso de apelación, la cual fue confirmada el 3 de septiembre del mismo año por el Segundo Tribunal Unitario del Primer Circuito, bajo el toca 70/98.