UNIVERSIDAD COMPLUTENSE DE MADRID

FACULTAD DE DERECHO

DEPARTAMENTO DE DERECHO PENAL

DELINCUENCIA INFORMÁTICA:

DAÑOS INFORMÁTICOS DEL ARTÍCULO 264 DEL CÓDIGO PENAL Y PROPUESTA DE REFORMA

TESIS DOCTORAL DE:

JORGE ALEXANDRE GONZÁLEZ HURTADO

BAJO LA DIRECCIÓN DE:

MARÍA TERESA REQUEJO NAVEROS

Madrid, 2013

UNIVERSIDAD COMPLUTENSE DE MADRID

FACULTAD DE DERECHO

Departamento de Derecho penal

TESIS PARA OBTENER EL TÍTULO DE DOCTOR EN DERECHO

DELINCUENCIA INFORMÁTICA: DAÑOS INFORMÁTICOS DEL ARTÍCULO 264 DEL CÓDIGO PENAL Y PROPUESTA DE REFORMA

Autor:

Jorge Alexandre González Hurtado

Directora:

Dra. María Teresa Requejo Naveros

Madrid, Mayo de 2013

TESIS PARA OBTENER EL TÍTULO DE DOCTOR EN DERECHO

DELINCUENCIA INFORMÁTICA: DAÑOS INFORMÁTICOS DEL ARTÍCULO 264 DEL CÓDIGO PENAL Y PROPUESTA DE REFORMA

Autor:

Jorge Alexandre González Hurtado

Directora:

Dra. María Teresa Requejo Naveros

Departamento:

Derecho penal

Miembros del Tribunal:

Presidente:

Secretario:

Vocal:

Vocal:

Vocal:

Madrid, Mayo de 2013

Mi sincero agradecimiento a mi directora Mª Teresa Requejo Naveros, por su desinteresado esfuerzo, y porque sin ella nada de esto sería posible.

Mi agradecimiento a la Facultad de Derecho de la Universidad Complutense de Madrid, mi hogar durante los últimos años, y a cada profesor que ha contribuido en mi formación.

Y, por supuesto, también a mis padres.

RESUMEN

El presente trabajo de investigación tiene como finalidad ofrecer una visión general de la delincuencia informática en la actualidad, centrando su análisis en el marco legal de los delitos de daños informáticos ubicados en el artículo 264 de la LO 10/1995 de 23 de noviembre, del CÓDIGO PENAL, artículo que ha sido sustancialmente modificado por la LO 5/2010 de 22 de junio, de reforma del Código penal.

ABSTRACT

On this dissertation we intend to make an overview of cybercrime in the present and analyze the legal regulation of the criminal offense of computer damage, legislated in the article 264 in the LO 10/1995 of November 23rd, in the SPANISH PENAL CODE, this article has been widely expanded by LO 5/2010 of June 22nd on the reform of the Spanish Penal Code.

ÍNDICE GENERAL

ABOUT THE RESEARCH 1

INTRODUCCIÓN 7

PRIMERA PARTE:

LA INFORMÁTICA Y LA DELINCUENCIA INFORMÁTICA EN ESPAÑA Y EN EL MUNDO

CAPÍTULO PRIMERO: LA INFORMÁTICA Y LOS ABUSOS COMETIDOS A TRAVÉS DE SISTEMAS INFORMÁTICOS

1. Introducción 19

2. Informática básica. Origen y evolución 20

A) El origen de la informática 21

B) La informática moderna 22

b.1. La aparición de los ordenadores personales 24

b.2. La aparición de las redes informáticas 26

C) Terminología en las actividades informáticas 29

c.1. Ordenador, sistema informático y redes de sistemas informáticos 31

c.1.1. Conceptos en torno a la idea de *hardware* 32

c.1.2. Conceptos en torno a la idea de *software* 33

c.1.3. Conceptos en torno a la idea de sistema informático y redes informáticas 33

c.2. *Hackers*, *crackers* y otros sujetos asociados a la informática 38

3. La informática como fuente de abusos 40

A) Historia de los virus informáticos 41

a.1. El primer virus informático y evolución de los virus 43

a.2. Los virus informáticos en la actualidad 45

a.2.1. Por la forma de propagación 46

a.2.2. Por el efecto en el sistema 48

a.2.3. Variantes combinadas 50

B) Otros ataques informáticos 51

b.1. Hacking web 51

b.1.1. Ataques de denegación de servicios o DDoS no intrusivos 52

b.1.2. Ataques para acceder a los servicios e información de otros sistemas 55

b.2. Hacking *wireless* 57

CAPÍTULO SEGUNDO: REGULACIÓN EN EL ÁMBITO INTERNACIONAL DE LA DELINCUENCIA INFORMÁTICA Y TRASCENDENCIA EN NUESTRO ESTUDIO

1. Introducción 59

2. Antes del Convenio y de la normativa de la UE: el nacimiento del Derecho penal informático 60

A) En el ámbito internacional 61

a.1. El papel de la Organización de Cooperación y Desarrollo Económico (OCDE) 61

a.2. El trabajo de la Organización de Naciones Unidas en la lucha contra la delincuencia informática 63

a.3. Otros instrumentos de Derecho Internacional 67

a.3.1. La recomendación R(89)9 del Consejo de Europa 67

a.3.2. Las Conferencias Internacionales de la Universidad de Wurzburgo 69

a.3.3. II Jornadas Internacionales sobre el Delito Cibernético 70

B) Regulaciones de ámbito nacional en países de nuestro entorno 72

b.1. Estados Unidos, primer país en tener una regulación de ámbito estatal 72

b.2. Las primeras regulaciones a nivel estatal en Europa. 77

C) Introducción a la regulación penal en España 80

c.1. Los primeros casos de delincuencia informática en España 82

3. Convenio sobre la Ciberdelincuencia de Budapest de 23 de noviembre de 2001 85

A) El preámbulo del Convenio y el capítulo primero 85

B) Capítulo segundo 88

b.1. Sección primera. Derecho penal sustantivo 88

b.2. Sección segunda y tercera. Derecho procesal y jurisdicción 91

C) Capítulo tercero. Cooperación internacional. 92

D) Capítulo cuarto. Disposiciones finales. 95

E) Protocolo sobre la incriminación de actos de naturaleza racista y xenófoba. 97

4. Movimientos reguladores en el ámbito europeo 98

A) Decisión 92/242/CEE del Consejo, de 31 de marzo, en materia de seguridad de los sistemas de información 98

B) COM(2000)890 final, de 26 de enero de 2001 100

C) Regulación penal de la Unión Europea en materia de delitos informáticos 103

c.1. Directiva 2011/93/UE del Parlamento Europeo y del Consejo, de 13 de diciembre de 2011 103

c.2. Decisión Marco 2005/222/JAI del Consejo, de 24 de febrero de 2005 106

c.2.1. La Decisión Marco. Unificación de criterios 106

c.2.2. Derecho penal sustantivo que impone la Decisión Marco 109

c.2.3. Otros extremos contenidos en la Decisión Marco 113

c.3. La propuesta de Directiva relativa a los ataques contra los sistemas de información 115

D) La Lucha contra la ciberdelincuencia en la Unión Europea en la actualidad 118

d.1. Comunicación acerca de dirigirse hacia una política general de lucha contra la ciberdelincuencia de 2007 118

d.2. Comunicación acerca de proteger Europa de ciberataques e interrupciones a gran escala de 2009.. 122

d.3. Comunicación sobre la protección de infraestructuras críticas de información de 2011 125

d.4. Comunicación sobre la represión del delito en la era digital y la creación de un centro europeo de ciberdelincuencia de 2012..... 131

5. Trascendencia en nuestro estudio. 134

A) Clasificación preliminar de los delitos informáticos 135

a.1. Delitos informáticos según establece la OCDE 136

a.2. Delitos informáticos según establece la ONU..... 138

a.3. Delitos informáticos según establece la Unión Europea 139

a.4. Delitos informáticos según establece el Convenio sobre la Ciberdelincuencia de Budapest de 23 de noviembre de 2001 141

a.5. Delitos informáticos conforme al Código penal de 1995 142

a.6. Delitos informáticos conforme a la clasificación de la Fiscalía General del Estado en España..... 146

B) El objeto concreto de nuestro estudio. Los daños informáticos 149

SEGUNDA PARTE:

LOS DELITOS DEL ARTÍCULO 264 DEL CÓDIGO PENAL. REGULACIÓN DE LOS DAÑOS INFORMÁTICOS EN ESPAÑA

CAPÍTULO TERCERO: ANÁLISIS JURÍDICO-PENAL DE LOS TIPOS DE DAÑOS INFORMÁTICOS DEL ARTÍCULO 264 DEL CÓDIGO PENAL

1. Introducción..... 153

2. Origen y evolución de los delitos de daños informáticos en España 155

A) Precedentes de la regulación de daños informáticos en España: el antiguo 264.2 CP 156

B) La reforma de los daños informáticos de 2010..... 158

b.1. La reforma desde el punto de vista legislativo. Cuestiones generales 158

b.2. La reforma de los daños informáticos del artículo 264 CP 167

C) Texto de la Comisión General de Codificación, del Proyecto de Ley y de la LO 5/2010 de 22 de junio 171

3. Análisis del tipo objetivo..... 176

A) Bien jurídico protegido en los daños informáticos..... 177

B) Acción típica..... 181

b.1. Elementos del artículo 264.1 CP 181

b.1.1. Las acciones de borrar y suprimir datos, programas informáticos o documentos electrónicos..... 182

b.1.2. La acción de hacer inaccesibles datos, programas informáticos o documentos electrónicos 186
b.1.3. La acción de alterar datos, programas informáticos o documentos electrónicos 190
b.1.4. La acción de deteriorar datos, programas informáticos o documentos electrónicos 194
b.1.5. La acción de dañar datos, programas informáticos o documentos electrónicos 195
b.1.6. La fórmula "por cualquier medio" 197
b.1.7. La gravedad en el medio y la gravedad en el resultado 199
b.1.8. La ajenidad y la falta de autorización 206
b.2. Elementos del artículo 264.2 CP 210
b.2.1. El uso de las fórmulas "por cualquier medio", "sin estar autorizado", "de manera grave" y con un "resultado producido grave" y la de "ajenidad" en el tipo del artículo 264.2 CP 210
b.2.2. Las acciones de interrumpir y de obstaculizar sistemas informáticos 212
b.2.3. Los modos de interrumpir y de obstaculizar sistemas informáticos 215
(a) Introducir o transmitir datos informáticos 215
(b) Dañar, borrar, deteriorar, alterar, suprimir o hacer inaccesibles datos informáticos 216
b.3. Modalidades comisivas 217
b.4. Grado de ejecución 222
b.5. Autoría y participación 225
C) Análisis de los sujetos 227
c.1. Sujeto activo 227
c.2. Sujeto pasivo 230
D) Objeto material 231
4. Análisis del tipo subjetivo 239
A) Tratamiento del dolo en los daños informáticos 239
a.1. El dolo en los delitos de daños informáticos 239
a.2. Elementos subjetivos del injusto 241
B) La imprudencia en los delitos de daños informáticos 242
5. Circunstancias modificativas que afectan a los daños informáticos 243
A) Agravantes genéricas y supuestos agravados 243
a.1. Agravantes genéricas del artículo 22 CP 243
a.2. Supuestos agravados. El apartado tercero del artículo 264 CP 245
a.3. Supuestos agravados. El apartado tercero del artículo 266 CP 247
B) Circunstancias que eximen total o parcialmente de responsabilidad penal 248
b.1. Causas de justificación 248
b.2. Causas de inimputabilidad 250
b.3. El miedo insuperable 251
b.4. Eximentes incompletas y atenuantes 251

b.5. El caso especial del artículo 268 CP. La excusa absolutoria 252

6. Problemas concursales 253

A) Casuística general 253

B) Pluralidad de afectados y delito continuado 256

7. Consecuencias jurídicas 257

A) Referencias a los marcos internacionales 257

B) La penalidad prevista en el Código penal 259

C) La falta del artículo 625.1 CP 261

TERCERA PARTE:

EVALUACIÓN DE LA ACTUAL REGULACIÓN DE DAÑOS INFORMÁTICOS Y DELITOS CONEXOS. PROPOSICIÓN DE UN MARCO LEGISLATIVO ALTERNATIVO

CAPÍTULO CUARTO: DUDAS QUE SUSCITA LA ACTUAL REGULACIÓN. CONSTRUCCIÓN DE UN BIEN JURÍDICO AUTÓNOMO: LA SEGURIDAD EN LOS SISTEMAS DE INFORMACIÓN

1. Introducción 265

2. Conflictos derivados de la persecución de las acciones delictivas 266

A) En el ámbito policial 267

B) En el ámbito procesal 269

3. Evaluación de la trasposición de la normativa internacional de daños informáticos 272

A) Trasposición de la normativa internacional 272

B) Puntos críticos de la trasposición. La difusión de virus informáticos y otras acciones similares 276

4. Principales dudas que se plantean en torno al actual modelo de regulación 278

A) Comisión por medios físicos o medios informáticos 278

B) Doble gravedad exigida en el tipo 280

C) Gravedad del resultado: el valor económico del daño informático 281

D) Enumeración de acciones: ¿literalidad o exceso? 285

E) El bien jurídico inmediatamente protegido 286

5. La modificación del actual punto de vista 288

A) La posible introducción de un Título o Capítulo en nuestro Código penal dedicado a la informática 288

a.1. Teoría del bien jurídico protegido en relación con los delitos informáticos 289

a.2. La seguridad informática desde otras ópticas dogmáticas. 298

B) Construcción del bien jurídico protegido en los delitos informáticos. La seguridad en los sistemas de información 299

b.1. La seguridad en los sistemas de información como bien jurídico digno de protección penal 301

b.2. Delitos informáticos que integran el nuevo bien jurídico protegido 305
b.2.1. Delitos en los que se manifiesta con mayor intensidad 306
b.2.2. Delitos en los que se manifiesta con menor intensidad 311
b.3. ¿La seguridad de los sistemas de información como manifestación del orden público? 313

CAPÍTULO QUINTO: PROPOSICIÓN DE UN MARCO LEGISLATIVO ALTERNATIVO PARA LOS DAÑOS INFORMÁTICOS Y DELITOS CONEXOS

1. Introducción 321

2. Ubicación en el Código penal 322

3. El Título relativo a los "delitos contra la seguridad en los sistemas de información" y su contenido 323

A) Tipos básicos 324
a.1. Acceso ilícito 324
a.2. Daño informático. 327
a.3. Sabotaje informático. 334
b.4. Abuso de dispositivos. 336
B) Supuestos agravados en los delitos contra la seguridad en los sistemas de información 339
C) Responsabilidad penal de las personas jurídicas 344
D) Otras reformas vinculadas 345

CONCLUSIONES DE LA INVESTIGACIÓN 351

BIBLIOGRAFÍA

Manuales, monografías y artículos citados 359
Otras fuentes 378

ÍNDICE DE LEGISLACIÓN 381

ÍNDICE DE JURISPRUDENCIA 385

RELACIÓN DE ABREVIATURAS UTILIZADAS

AIDP:	Asociación Internacional de Derecho Penal
ARC:	Augmentation Research Center
ARPANET:	Advanced Research Projects Agency Network
BIT:	Brigada de Investigación Tecnológica
BJA:	Bureau of Justice Assistance
CE:	Constitución Española
CEPOL:	Collège Européen de Police
CERN:	Conseil Européen pour la Recherche Nucléaire
CERT:	Computer Emergency Response Team
CNI:	Centro Nacional de Inteligencia
CNSS:	Comitte On National Security System
CP:	Código Penal
CSI:	Computer Secure Institute
COM:	Comunicación (de la Unión Europea)
DDoS:	Distributed Denial of Service
DUDH:	Declaración Universal de los Derechos Humanos
EC3:	European CyberCrime Centre
ECCP:	European CyberCrime Platform
EEUU:	Estados Unidos
EFMS:	European Forum for Member States
EISAS:	European Information Sharing and Alert System
ENIAC:	Electronic Numerical Integratos and Calculator
ENISA:	European Network and Information Security Agency
EP3R:	European Public-Private Partnership for Resilience
FAT:	File Allocation Table
FBI:	Federal Bureau of Investigation
FTP:	File Transfer Protocol
GDI:	Grupo de Delitos Informáticos
GDT:	Grupo de Delitos Telemáticos
IC3:	Internet Crime Complaint Center
ICCP:	Information, Computer and Communications Policy
IEEE:	Institute of Electrical and Electronics Engineers
IFCC:	Internet Fraud Complaint Center
INTECO:	Instituto Nacional de Tecnologías de la Comunicación
LECrim:	Ley de Enjuiciamiento Criminal
LG:	Ley del Gobierno

LO:	Ley Orgánica
NASA:	National Aeronautics and Space Administration
OCDE:	Organización de Cooperación y Desarrollo Económico
ONU:	Organización de Naciones Unidas
PYME:	Pequeña y Mediana Empresa
R:	Recomendación (de la Unión Europea o del Consejo de Europa)
RAE:	Real Academia Española
SAP:	Sentencia de la Audiencia Provincial
STC:	Sentencia del Tribunal Constitucional
STEDH:	Sentencia del Tribunal Europeo de Derechos Humanos
StGB:	Strafgesetzbuch (Código penal alemán)
STJCE:	Sentencia del Tribunal de Justicia de las Comunidades Europeas
STS:	Sentencia del Tribunal Supremo
TCP:	Transmission Control Protocol
TEDH:	Tribunal Europeo de Derechos Humanos
TIC:	Tecnología de la información y la comunicación
UE:	Unión Europea
UNED:	Universidad Nacional de Educación a Distancia
USA:	United States of America
WPISP:	Working Party on Information Security and Privacy
WWW:	World Wide Web

ABOUT THE RESEARCH

In the pages that can be analyzed we will try to guide the reader in the direction that has marked the legislator to regulate certain types of crimes related to new technologies that have been unprecedented in our criminal law until less than two decades. No doubt that at the moment of history in which we find new technologies have played a key role, both for his role in the daily lives of the people and its important role in the economic and social sector. All countries, in the exercise of their executive and legislative powers have been trying over the last three decades to create a legal framework closely related to computers and new technologies. But not only the Public Sector has joined the use of new technologies; electronic commerce is overcoming the barriers imposed by a society that mistrusts classical changes and is becoming increasingly common practice, which is expected to eventually replace the traditional trade.

Much has been developed on the field in the network security through different techniques, but cannot forget that such developments do not prevent the emergence of new forms of criminality linked to technological progress. New subjects have appeared willing to use to their advantage in this world that, despite the time elapsed, it seems that is still taking its first steps. So, short of asserting that the law of computing is the most innovative branches of law, no doubt, already takes a very high position of prominence among the areas of law, both for its fast expansion and its transversality, affecting all areas of knowledge. We can say, without fear of error, which was totally unthinkable that such expansion in the computer law also did not occur in the criminal field, making certain changes that are having an increasing role.

The significance of any of these changes, from the position taken by the international community and, specifically, the specific regulation of computer damage in Spain, will be the central object of our analysis throughout this research. These computer-related crimes, in particular, have suffered extensive modification in the Spanish criminal system, which has led them to be mere marginal offenses, often without autonomy and in direct dependence to others, to become an important

separate crimes relevant that makes them worthy of a larger study than they have had. Certain types of crimes that are currently under construction, as is the case of computer damage offenses punishable under Article 264 of the Spanish Criminal Code, which will be erected in research-axis, are going to be turned into real protagonists of the criminal law before the end of this decade, as they have come to be, since the beginning of the century in the field of computer security and telecommunications. The new text of Article 264 of the Spanish Criminal Code, drafted by the reform made by the Organic Law 5/2010 of June 22, provides a framework developed remarkably in comparison with the computer damage that was done in the previous legislation.

On the structure of research we can advance the development of the second and third chapters, intended to detail the criminal regulations about computer abuse, will try to fix the origin of criminal regulation of these figures and then get into the Spanish legislation. Analyze the Convention on Cybercrime of the Council of Europe in Budapest on November 23, 2001, which has established itself as the best tool for the participating States in the fight against cybercrime, and the Framework Decision 2005/222/JHA of Council of the European Union of 24 February, which is the basic tool that has led to the current criminal regulation in our country. In the third chapter, also we will initiate criminal legal analysis of the figures contained in the Spanish Criminal Code relating to computer damage, this will be a key part of the contents of this research. We will analyze the legally protected, the elements of the criminal action (we will see, there are many), the methods of perpetration, the analysis of the subjects, the subjective element, the modifying circumstances, etc. We recognize that due to the extensive that it can become the subject matter of study other aspects are considerably limited despite of their linkage could have been equally treated in this study. This way, a detailed analysis of legal and criminal related offenses, or with which usually appear the aforementioned computer damage, such as the crime of illegal access to information systems, as specified in Article 197.3 of the Criminal Code, introduced same reform has modified our Article 264, or the regulation of Article 248.2 of computer fraud will not be made. In any case clarifications and references will be made when necessary for better understanding of the research. The fourth and fifth chapters, which ends the research before enunciate the conclusions,

will try to bring out the real situation of cybercrime in contrast to the criminal framework established. Check the current problems faced by the regulation as applied by operators of law and by the Force Enforcement Agencies of the State, and the solutions we can seek to mitigate these negative effects of regulation. The fifth chapter concludes with a proposed new framework for criminal damage offenses and computer related actions. This proposal, although it is within the ambit of the last chapter, attempts to answer the problems that have been breaking out along the research, so it can become a reference for the legislator in the future.

Finally about the structure of the research, we must warn the reader that with the development of this work we have been raiding various problems of terminology used at the criminal offenses that we will now analyze. It is important to know the proper language of science we treat, whose transcendence is even greater when we move into the field of criminal law, in which the literal and strictly of the precepts works as a guiding principle, especially now, since in the issues before us, many times, it is difficult to draw the line between the common concept of a word and its technician meaning. Added to this, and unfortunately, there isn't a dictionary of computer terms, or better said, there are as many as we can imagine. Although it will be attempted along the following pages, where appropriate, the basic information to correctly understand each concept we use, the truth is that there is not always unified criteria for accurately determining the scope and content of some words. Therefore, we have dedicated the first chapter to these problems. We believe that the scope and issues raised by the subject matter of this research exceeds the strictly legal-dogmatic limits, so we will give the minimum development that deserves to other important issues that are inextricably linked with the figure of computer damage. First, we believe it is appropriate to make a dedicated historical introduction to computing that allows us to assess the complexity of science with which we find ourselves. Alongside this historical approach, we analyze from a general point of view, but large enough, computer behavior may be called abusive or socially reprehensible, so that we know well the worst side of the computer world. This first chapter was the last to be developed, although not, as will be understood, the focus of the investigation, should the reader be conveniently located within margins that know and appreciate that without doubt it is essential to expose for a full understanding of

the problem to which we face. In order not to turn away in excess of legal topics, along the same we will be giving the first strokes associated with its subsequent impact on the analysis of criminal offenses. So reading beyond be a source of useful information for anyone interested both, from a legal perspective as foreign to the world of law, and necessary to correctly understand the rest of the investigation.

Regarding the conclusions of the research we note as most important idea that now both institutions, whether public or private, as individuals, and all kinds of associations, take whatever form, are inevitably doomed the use of computers and information systems. It is simply inevitable. It seems difficult to return to a previous stage as it has been producing the evolution of society. Like it or not, this is the way it has been chosen to follow. However, the introduction into society of new tools designed to make people's lives more comfortable, means that they can be used completely opposite purposes for which they were created, alert to them must always be public authorities, both nationally and internationally. In the development of this research the conclusion is drawn that have been put in place the legal -and police- appropriate measures to protect society from a new type of crime, both in the international concert, which is essential, as in our domestic. However, the regulation was made in Spain for crimes of computer damage, even may be enough at the present time and is in line with most of the international commandments and similar to that of neighboring countries, can be reformulated from new integrative principles. The literal construction articles show some doubts of interpretation, and in the current jurisprudence no answer for the lack of cases brought before the courts, because the existence of these crimes become known is still limited. Scholars also have not had the opportunity to express it extensively. The success of having been aware of the new problems appeared with the development of new technologies, should not blur of cumbersome regulation, and difficult to interpret. While it has started down the path to protect society from new types of crime, it is necessary to do with maximum effectiveness.

Therefore, from the recognition that we profess in the implementation of concrete measures both national and international, should be encouraged to maintain the current effort to complete to the best of our legal system in relation to new technologies, especially in criminal matters.

Main bibliography:

ÁLVAREZ GARCÍA, Francisco Javier y GONZÁLEZ CUSSAC, José Luis (dirs.): *Comentarios a la Reforma Penal 2010,* Ed. Tirant lo Blanch, 1ª edición, Valencia, 2010.

ANDRÉS DOMÍNGUEZ, Ana Cristina: *El Delito de Daños: Consideraciones Jurídico-Políticas y Dogmáticas*, Ed. Universidad de Burgos, 1ª edición, Burgos, 1999.

ANDRÉS DOMÍNGUEZ, Ana Cristina: "Los daños informáticos en el Derecho penal europeo" en ÁLVAREZ GARCÍA, Francisco Javier; MANJÓN-CABEZA OLMEDA, Araceli y VENTURA PÜSCHEL, Arturo (coords.): *La adecuación del Derecho penal español al ordenamiento de la Unión Europea*, Ed. Tirant lo Blanch, 1ª edición, Valencia, 2009.

ARNALDO ALCUBILLA, Enrique.: "El orden público y la seguridad ciudadana en la Constitución española de 1978" en *Cuadernos de Seguridad y Policía*, nº 7, 2011.

BARRIO ANDRÉS, Moisés: "El régimen jurídico de los delitos cometidos en Internet en el derecho español tras la reforma penal de 2010", en *Delincuencia informática. Tiempos de cautela y amparo,* Ed. Thomson Reuters Aranzadi, 1ª edición, Navarra, 2012.

DAVARA RODRÍGUEZ, Miguel Ángel: *Manual de Derecho Informático*, Ed. Thomson Aranzadi, 10ª Edición, Navarra, 2008.

DE LA CUESTA ARZAMENDI, José Luis y DE LA MATA BARRANCO, Norberto Javier: *Derecho Penal Informático,* Ed. Thomson Reuters, 1ª edición, Navarra, 2010.

FARALDO CABANA, Patricia: *Las nuevas técnologías en los delitos contra el patrimonio y el orden socioeconómico*, Ed. Tirant lo Blanch, 1ª edición, Valencia, 2009.

FERNÁNDEZ TERUELO, Javier Gustavo: *Cibercrimen. Los delitos cometidos a través de internet*, Ed. Constitutio Criminalis Carolina, 1ª edición, Oviedo, 2007.

FLORES PRADA, Ignacio: *Criminalidad Informática. Aspectos sustantivos y procesales*, Ed. Tirant lo Blanch, 1ª edición, Valencia, 2012.

GARCÍA MEXÍA, Pablo: *Principios de Derecho de Internet*, Ed. Tirant lo Blanch, 2ª edición, Valencia, 2005.

GONZÁLEZ RUS, Juan José: "Los ilícitos en la red (I): hackers, crackers, cyberpunks, sniffers, denegación de servicio y otros comportamientos semejantes" en ROMEO CASABONA, Carlos María (dir.): *El cibercrimen, nuevos retos jurídico-penales, nuevas respuestas político criminales*, Ed. Comares, Granada, 2006.

GUTIÉRREZ FRANCÉS, María Luz.: "Delincuencia económica e informática en el nuevo Código Penal", en GALLARDO ORTIZ, Miguel Ángel: *Ámbito jurídico de las tecnologías de la información*, Ed. CGPJ, 1ª edición, Madrid, 1996.

MARCHENA GÓMEZ, Manuel: "El sabotaje informático: entre los delitos de daños y los desórdenes públicos*"* en *Internet y Derecho penal. Consejo General del Poder Judicial*, número 10, Madrid, 2001.

MATA y MARTÍN, Ricardo Manuel: *Delincuencia informática y derecho penal* Ed. Edisofer, 1ª edición, Madrid, 2001.

MIR PUIG, Santiago: *Delincuencia Informática*, Ed. PPU, 1ª edición, Barcelona, 1992.

O'REGAN, Gerard: *A brief history of computing*, Ed. Springer, 1ª edición, Londres, 2010.

ROMEO CASABONA, Carlos María, GUANARTEME SÁNCHEZ LÁZARO, Fernando y ARMAZA ARMAZA, Emilio José (coords.): *La adaptación del Derecho penal al desarrollo tecnológico*, Ed. Comares, 1ª edición, Granada, 2010.

ROVIRA DEL CANTO, Enrique: *Delincuencia informática y fraudes informáticos*, Ed. Comares, Granada, 2002.

SANTA CECILIA GARCÍA, Fernando.: *Delito de daños. Evolución y dogmática (art. 263 Código penal)*, Ed. Universidad Complutense de Madrid, 1ª edición, Madrid, 2003.

SUÑÉ LLINÁS, Emilio: *Tratado de Derecho Informático Volumen I*, Ed. Complutense, 1ª edición, Madrid, 2002.

VELASCO NÚÑEZ, Eloy (dir.): *Delitos contra y a través de las nuevas tecnologías. ¿Cómo reducir su impunidad?*, Ed. Consejo General del Poder Judicial, Cuadernos de Derecho Judicial, 1ª edición, Madrid, 2006.

INTRODUCCIÓN

En las páginas que se podrán analizar a continuación se va a tratar de orientar al lector en la dirección que ha marcado el legislador a la hora de regular ciertos tipos penales relacionados con las nuevas tecnologías que han sido inéditos en nuestro Derecho penal hasta hace poco menos de dos décadas. Todo ello sin olvidar que tales acciones penales tienen su origen y razón de ser en la imparable evolución de la informática en los últimos setenta años, y muy especialmente a partir de la década de 1980.

No cabe duda de que en el momento de la historia en el que nos encontramos las nuevas tecnologías han ocupado un papel fundamental, tanto por su implicación en la vida diaria de las personas como por su importante papel en el sector económico y social[1]. Los Estados, en el ejercicio de sus potestades ejecutivas y legislativas se han ido procurando a lo largo de las últimas tres décadas de un marco legal estrechamente relacionado con la informática y las nuevas tecnologías. Esto es lo que una parte de la doctrina[2], que parece ser la más acertada, ha venido a denominar como Derecho de la informática, entendido como la rama del derecho que

[1] CORCOY BIDASOLO, M.: "Problemática de la persecución penal de los denominados delitos informáticos: particular referencia a la participación criminal y al ámbito espacio temporal de comisión de los hechos" en *Eguzkilore: cuaderno del Instituto Vasco de Criminología*, nº 21, 2007, p. 8, "la informática constituye un instrumento indispensable en todos los ámbitos de actividad. Tanto la organización y administración de empresas y administraciones públicas, como la investigación científica, la producción industrial o el estudio y la investigación, e incluso el ocio, necesitan de la informática". En el mismo sentido, ADÁN DEL RÍO, C.: "La persecución y sanción de los delitos informáticos" en *Eguzkilore: Cuaderno del Instituto Vasco de Criminología*, nº 20, 2006, p. 152, manifiesta con todo el sentido común que "hoy en día, pocos ciudadanos viven al margen o sin contacto directo o indirecto con un medio informático […] De hecho, no resulta exagerado afirmar que de cara al futuro generamos una dependencia creciente a estos medios, siendo su incorporación a nuestra vida cotidiana, algo tan evidente, que pronto ésta se verá notablemente dificultada sin su apoyo". Desde una perspectiva negativa, LEZERTUA RODRÍGUEZ, M.: "El Proyecto de Convenio sobre el cibercrimen del Consejo de Europa - proteger el ejercicio de derechos fundamentales en las redes informáticas" en *Cuadernos europeos de Deusto*, nº 25, 2001, p. 84, "a medida que se incrementa nuestra dependencia de las redes informáticas globales, se hace más evidente la vulnerabilidad de los usuarios".

[2] SUÑÉ LLINÁS, E.: *Tratado de Derecho Informático Volumen I*, Ed. Complutense, 1ª edición, Madrid, 2002, p. 3. "Aunque la mayor parte de los autores empleen como sinónimas las expresiones Derecho Informático y Derecho de la Informática, para mí no lo son […] El Derecho Informático […] es la disciplina que engloba a la Informática Jurídica y al propio Derecho de la Informática".

tiene por objeto regular todos aquellos ámbitos en los que los sistemas informáticos se encuentran presentes[3].

Pero no sólo los Estados se han sumado al uso de las nuevas tecnologías. El comercio electrónico va superando las barreras impuestas por una sociedad clásica que desconfía de los cambios -cuyas dudas sobre los nuevos modos de actuar no son siempre infundadas- y está convirtiéndose cada día más en una práctica habitual, de la que cabe esperar que tarde o temprano sustituya completamente al comercio tradicional[4]. Mucho se ha desarrollado el campo relativo a la seguridad en la red a través de diferentes técnicas, pero no podemos olvidar que tales avances no impiden la aparición de nuevas formas de criminalidad sujetas al propio progreso tecnológico[5]. Han aparecido nuevos sujetos que están dispuestos a utilizar en su beneficio (entendido en un sentido amplio) este mundo que, a pesar del tiempo transcurrido, parece que todavía sigue dando sus primeros pasos[6].

Sin llegar a afirmar que "el Derecho de la informática es la más innovadora de las ramas del Derecho"[7] no cabe duda de que ocupa ya un puesto de muy elevado protagonismo entre las ramas jurídicas, tanto por su rápida expansión como por su transversalidad[8], al afectar a materias de todos los ámbitos[9]. Y desde ahí volvemos al

[3] La definición aportada no tiene discusión en la doctrina aunque se puede afirmar que se trata de un concepto muy general, tanto en lo referente a sistemas informáticos, que se debe entender en el sentido más amplio, incluidos prácticamente todos los equipos que guarden relación con las nuevas tecnologías; como en la expresión referida a los ámbitos donde se encuentran presentes, que son, hoy en día, prácticamente todos.

[4] GUTIÉRREZ FRANCÉS, M. L.: "Reflexiones sobre la ciberdelincuencia hoy. En torno a la ley penal en el espacio virtual" en *Revista electrónica del departamento de derecho de la Universidad de La Rioja, REDUR*, nº 3, 2005, pp. 70 y 71.

[5] Con diferentes nomenclaturas como ciberdelitos, cibercrimen, etc. ROMEO CASABONA, C. M.: "De los delitos informáticos al cibercrimen, una aproximación conceptual y político criminal" en ROMEO CASABONA, C. M. (dir.): *El cibercrimen, nuevos retos jurídico-penales, nuevas respuestas político criminales*, Ed. Comares, Granada, 2006, pp. 7 y ss. También en ROMEO CASABONA, C. M.: "De los delitos informáticos al cibercrimen" en PÉREZ ÁLVAREZ, F. (ed.): *Homenaje a Ruperto Núñez Barbero*, Ed. Universidad Salamanca, 1ª edición, 2007.

[6] VÁZQUEZ IRUZUBIETA, C.: *Manual de Derecho Informático*, Ed. Dijusa, 1ª edición, Madrid, 2002, p. 634.

[7] Así lo afirma SUÑÉ LLINÁS, E.: *Tratado…* ob. cit. p. 8.

[8] En este sentido SUÑÉ LLINÁS, E.: *Tratado…* ob. cit. pp. 11 y 12, señala que "el Derecho de la Informática es poco acomodaticio a los moldes tradicionales del Derecho". Afirma también que a diferencia de las ramas clásicas que son verticales, el Derecho de la Informática se configura de manera horizontal. Se refiere este autor a que mientras las ramas clásicas del Derecho aglutinan

tema central que ocupa esta incipiente investigación. Podemos afirmar sin miedo a equivocarnos que resultaba totalmente impensable que dicha expansión del Derecho de la Informática no se produjese también en el ámbito penal[10], operando ciertos cambios que cada vez tienen mayor protagonismo[11].

La trascendencia de alguno de estos cambios desde la posición que ha tomado la Comunidad Internacional y, específicamente, la regulación concreta relacionada con los daños informáticos en nuestro país, será el objeto central de nuestro análisis a lo largo de esta investigación[12]. Estos delitos relacionados con la informática, en concreto, han sufrido una intensa modificación que los ha llevado de ser meros tipos marginales, a menudo sin autonomía y en dependencia directa con otros[13], a convertirse en tipos autónomos con una importancia relevante que los hace dignos de un estudio más amplio y detenido del que han recibido hasta ahora. Ciertos tipos penales que actualmente se están construyendo, como es el caso de los delitos de

---

contenidos que se han entendido como comunes, el Derecho de la Informática no lo hace, sino que conoce de casi cualquier rama tradicional: existe un Derecho administrativo de la Informática, un Derecho civil de la Informática, un Derecho penal de la Informática, etc. Es decir, su unidad no se produce por razón de la materia, sino del medio utilizado.

[9] Es ilustrativa la enumeración, que no debemos entender como cerrada, que realiza DAVARA RODRÍGUEZ, M.A.: *Manual de Derecho Informático*, Ed. Thomson Aranzadi, 10ª Edición, Navarra, 2008, pp. 27 y ss., en la que sitúa, entre otras, materias propias del ámbito civil, penal, laboral o administrativo: derechos de autor, cuestiones relativas al consumidor, protección de datos, operaciones relativas a las transferencias electrónicas de fondos entre diversos países, delitos informáticos, el papel del Estado en el desarrollo de las telecomunicaciones, etc.

[10] Lo que para PALOMINO MARTÍN, J. M.: *Derecho penal y nuevas tecnologías. Hacia un sistema informático para la aplicación del Derecho penal*, Ed. Tirant lo Blanch, 1ª edición, Valencia, 2006, pp. 62 y ss., se debe considerar el Derecho penal informático, diferente aunque irremediablemente vinculado al Derecho internacional informático y al Derecho procesal informático.

[11] Sobre una desmesurada expansión y creación de nuevas figuras innecesarias y otros excesos que pueden surgir de esta imprescindible adaptación del Derecho a las nuevas tecnologías habla GALÁN MUÑOZ, A.: "La internacionalización de la represión y la persecución de la criminalidad informática: un nuevo campo de batalla en la eterna guerra entre prevención y garantías penales" en *Revista penal*, nº 24, 2009, pp. 105 y ss. y GARCÍA GARCÍA-CERVIGÓN, J.: "Daños informáticos. Consideraciones penales y criminológicas" en *Actualidad Jurídica Aranzadi*, nº 588, 2003 (edición electrónica sin numerar).

[12] Los delitos informáticos han sido considerados por la doctrina americana como delitos de cuello blanco (*white collar crimes*). Bajo esta denominación, escasa en la doctrina continental, realiza una visión político criminal NÚÑEZ FERNÁNDEZ, J.: "Algunos aspectos conceptuales y políticos de la criminalidad de cuello blanco" en *Cuadernos de Política Criminal*, nº 71, 2000, pp. 523 y ss.

[13] Sin ir más lejos baste ver la anterior regulación de los daños informáticos (antiguo 264.2 CP en relación con el antiguo 263 CP), o la figura de acceso ilícito a sistemas informáticos del nuevo artículo 197.3 CP, inexistente hasta la reforma penal de 2010.

daños informáticos tipificados en el artículo 264 CP, que va a erigirse en eje de la investigación y que encuentra una escasa aplicación práctica en nuestros tribunales en la actual realidad procesal, se van a ver convertidos en auténticos protagonistas de la esfera penal antes del final de esta década[14] como ya lo han venido siendo, desde principios de siglo, en el ámbito de la informática y las telecomunicaciones[15].

El nuevo texto del artículo 264 del Código penal español, producto de la reforma operada por la LO 5/2010 de 22 de junio de Reforma del Código penal, establece un marco notablemente desarrollado en comparación con la tipificación que de los llamados daños informáticos se hacía en la anterior regulación[16]. La selección del artículo 264 del Código penal objeto de análisis responde al interés propio en el estudio de ciertas situaciones a las que nuestra extensa doctrina penalista

[14] VELASCO NÚÑEZ, E.: *Delitos cometidos a través de Internet. Cuestiones procesales*, Ed. La Ley, 1ª edición, Madrid, 2010, p. 44, señala, desde un punto de vista sociológico, que "estos delitos tienen una enorme proyección de futuro, ya que, por un lado, crecen desmesuradamente año a año […], y por otro, sus autores, en la mayor parte de los casos conocidos, son personas jóvenes que no alcanzan la media de los 50 años". En concreto, sobre los daños informáticos, la Memoria de la Fiscalía General del Estado del año 2012 señala que "aun cuando el número de estas investigaciones, por el momento, no es muy elevado, circunstancia en la que puede influir su reciente tipificación específica en el CP, es previsible su incremento en un futuro próximo, al hilo de la progresiva especialización en el manejo de las nuevas tecnologías y de la utilización de las mismas como medio de causar daño o perjuicio a otros por motivos de muy distinta naturaleza".

[15] Es habitual encontrar referencias a los delitos informáticos o el cibercrimen desde ópticas poco o nada jurídicas en publicaciones del sector de las TICs: LARKIN, E.: "Cibercrimen. Delincuentes profesionales online" en *Pc World*, nº 224, 2005, pp. 26 y ss., GONZÁLEZ, E.: "El cibercrimen, una amenaza en ciernes" en *Pc World*, nº 251, 2008, pp. 88 y ss. o HERNÁNDEZ CALLEJA, R.: "Cibercrimen, crónica de un auge anunciado" en *Pc World*, nº 269, 2009, pp. 10 y 11.

[16] Según algunos autores estas nuevas prácticas delictivas no suponen una novedad en sí mismas, sino más bien una novedad en el medio empleado (la informática) gracias al cual se cometen figuras delictivas clásicas. De esta opinión son MUÑOZ MACHADO, S.: *La regulación de la red, Poder y derecho en internet*, Ed. Taurus, 1ª edición, Madrid, 2000, p. 41, que señala que "muchas de estas situaciones jurídicamente problemáticas no son, en verdad, nuevas"; LAGARES GARCÍA, D.: *Internet y Derecho*, Ed. Carena, 1ª edición, Barcelona, 2000, p. 51, afirma que "no hay nada nuevo bajo el sol" o MARCHENA GÓMEZ, M., "Jurisdicción e Internet", en *Conferencia XV años de encuentro sobre Informática y Derecho*, Ed. Universidad Pontificia Comillas, Madrid, 2001, que sentencia que "los delitos cibernéticos son delitos típicos realizados mediante Internet". En la tercera parte de esta investigación se desarrollará una idea que tratará de discutir esta visión, baste ahora señalar las llamativas palabras que encontramos en ANDRÉS DOMÍNGUEZ, A.C.: *El Delito de Daños: Consideraciones Jurídico-Políticas y Dogmáticas*, Ed. Universidad de Burgos, 1ª edición, Burgos, 1999, p. 111, que señala que no puede "dejar de manifestar su asombro ante la inclusión en un mismo precepto de supuestos tan dispares como son los daños cometidos sobre un rebaño de ovejas y los ejecutados sobre un programa de ordenador". Aunque esta situación se ha corregido con la actual regulación, se insiste en la idea de que "no cabe duda que en la sociedad actual los ataques a los sistemas informáticos merecen sanción penal expresa pero, en nuestra opinión, no en sede de daños".

no ha dedicado demasiadas líneas[17]. No es un secreto que el desarrollo de las nuevas tecnologías en las dos últimas décadas se ha producido con una velocidad vertiginosa, y situaciones impensables hasta hace poco tiempo se producen hoy en día con, cada vez, mayor frecuencia[18]. Esta investigación, como ya hemos avanzado, se centra en los tipos penales del artículo 264 CP, de los que poco a poco se va encontrando una creciente y real repercusión en la práctica jurídica[19] a pesar de algunos hándicaps que los rodean, pudiendo señalar, de forma muy general, al menos dos de ellos: el primero es que las acciones que pueden ser incluidas en estos tipos penales se producen -por el momento- con escasa frecuencia en la sociedad actual, o al menos es poca la frecuencia de los casos en los que los afectados son conscientes de estar siendo víctimas de una acción delictiva[20]; el segundo motivo es que las acciones perseguibles que se puedan producir, a menudo quedan restringidas al ámbito privado de los afectados, pues desconocen la protección que el ordenamiento jurídico les ofrece, o esa protección es insuficiente o, a la hora de la verdad, inexistente y por lo tanto la descartan[21]. Pocos son los casos en los que los hechos

[17] Como se podrá ver a lo largo de la investigación, se puede afirmar que existen muchas referencias a este tipo penal en la doctrina (en su mayor parte concernientes al artículo 264.2 CP anterior a la reforma de 2010), especialmente conectadas con las dudas que se plantean en torno a la ubicación de la delincuencia informática en el Código. En cambio, son escasos los trabajos en profundidad sobre esta materia.

[18] De la Memoria de la Fiscalía General del Estado del año 2011, en su parte relativa a los delitos informáticos, se extraen algunos datos interesantes: La Fiscalía ha tenido conocimiento de 1.568 denuncias relacionadas con delitos informáticos, por las 399 denuncias señaladas en la Memoria del año anterior. En la Memoria de 2012 se ha iniciado un nuevo método de valoración de la criminalidad informática, por lo que en ella misma se advierte de no utilizar las cifras dadas para realizar comparaciones con años anteriores; en concreto, partiendo de procedimientos incoados en las diferentes fiscalías provinciales, el total llega a 6.532 procedimientos.

[19] La Memoria de la Fiscalía General del Estado del año 2012 señala que sólo un 1% de los procedimientos incoados en relación con los delitos informáticos suponen acciones de daños informáticos.

[20] Puede resultar necesario aquí recordar que la inseguridad ciudadana real, por diversos motivos, no siempre es la reflejada en las sensaciones de la ciudadanía, véase ZUGALDÍA ESPINAR, J. M.: "Seguridad ciudadana y Estado social de Derecho (A propósito del Código penal de la Seguridad y el pensamiento funcionalista)" en OCTAVIO DE TOLEDO Y UBIETO, E.; GURDIEL SIERRA, M. y CORTÉS BECHIARELLI, E. (coords.): *Estudios penales en recuerdo del profesor Ruiz Antón*, Ed. Tirant lo Blanch, 1ª edición, Valencia, 2004, p. 1122.

[21] DÍAZ GÓMEZ, A.: "El delito informático, su problemática y la cooperación internacional como paradigma de su solución: El Convenio de Budapest" en *REDUR*, nº 8 - diciembre, 2010, p. 181, se hace eco de estas dudas en las víctimas, especialmente empresas, señalando que "los procedimientos penales a menudo no se desean por miedo a que la reputación de las empresas resulte dañada, y se

regulados en el artículo 264 CP tienen una verdadera trascendencia social[22], pero no cabe duda de que esos pocos casos van a aumentar en los próximos años con una sociedad cada vez más interconectada e irremediablemente más mercantilizada. Es labor de las instituciones de los Estados procurar una protección real ante estos ataques, y no limitarse a defender con la letra de la ley comportamientos que no son capaces de repeler en la práctica real.

Sobre la estructura de la investigación podemos avanzar que el desarrollo de los capítulos segundo y tercero pretende profundizar sobre la regulación penal en torno a los abusos informáticos, partiendo de la fijación del origen (internacional) de la regulación penal de estas figuras para luego adentrarnos en la normativa española. Analizaremos el Convenio sobre la Ciberdelincuencia del Consejo de Europa de Budapest de 23 de noviembre de 2001, que se ha consolidado como la mejor herramienta de trabajo para los Estados participes en la lucha contra la delincuencia informática; y la Decisión Marco 2005/222/JAI del Consejo de la Unión Europea de 24 de febrero, que es el instrumento básico que ha motivado la actual regulación penal en nuestro país.

---

ocultan los delitos a las autoridades". En la misma línea CONTRERAS CLUNES, A.: "Delitos informáticos: un importante precedente" en *Ius et Praxis*, vol. 9, nº 1, 2003, p. 520, señala como excepcional, en un caso de daño informático en Chile, que "existió una empresa que se atrevió a denunciar el delito, con todas las consecuencias que trajo para con sus clientes y prestigio, algo que por lo general no hacen las víctimas de estos delitos". También SÁNCHEZ BRAVO, A. A.: "El Convenio del Consejo de Europa sobre cibercrimen: control VS. libertades públicas" en *Diario La Ley*, nº 5528, 2002, p.2.

[22] Con la aprobación en el Congreso de los Diputados del Proyecto de Ley de Economía Sostenible en el año 2010 (a la postre Ley 2/2011, de 4 de marzo, de Economía Sostenible) se pudo observar como un grupo de activistas informáticos inutilizaron las páginas web del Congreso, el Senado y los Partidos Políticos que apoyaron dicha ley. Lo cierto es que tales acciones, que pudieron suponer la existencia de un delito del artículo 264.2 CP, debieron haber sido motivo de una labor de investigación por parte de los Cuerpos y Fuerzas de Seguridad del Estado y la Fiscalía pero, finalmente, dichos asuntos parecen haberse cerrado sin que, hasta la fecha, se haya procedido penalmente contra los autores. Otro caso reciente, de un ataque a la plataforma de juego *online* propiedad de Sony, que ha supuesto la obstaculización del sistema que ha podido generar una cuantiosa pérdida económica para la compañía, se configura como una acción que no sólo afecta a la competencia y los consumidores, sino que supone la infracción de un precepto penal que obliga al Estado a actuar e investigar. En este caso se manifiesta a la vez uno de los problemas de este tipo de delitos ya que si bien el sujeto pasivo es la compañía, con sede en el extranjero, existen múltiples perjudicados en nuestro territorio; además de ello, la localización de los atacantes sigue suponiendo una incógnita, con los problemas policiales, procesales y de jurisdicción que ello conlleva.

En el capítulo tercero, además, daremos paso al análisis esencialmente jurídico-penal de las figuras recogidas en el Código penal relativas a los daños informáticos, ésta será una parte fundamental del contenido de la presente investigación. Se analizará el bien jurídico protegido, los elementos de la acción típica (que veremos, no son pocos), las modalidades comisivas, el análisis de los sujetos, el tipo subjetivo, las circunstancias modificativas, etc.

Debemos reconocer que debido a lo extensa que puede llegar a ser la materia objeto de estudio se limitan considerablemente otros aspectos que por su vinculación podrían haber sido igualmente tratados en este estudio. De esta forma, no se realizará un análisis jurídico-penal pormenorizado de otros delitos conexos, o junto a los cuales suelen aparecer los citados daños informáticos, como puede ser el delito de acceso ilícito a sistemas de información, regulado en el artículo 197.3 del Código penal, introducido en la misma reforma que ha modificado nuestro 264 CP, o la regulación de las estafas informáticas del artículo 248.2 CP, sin que eso sirva de excusa para que sobre ellos se hagan aclaraciones y referencias cuando sea necesario para la mejor comprensión de la investigación.

Los capítulos cuarto y quinto, con los que se pone fin a la investigación antes de enunciar las conclusiones, van tratar de poner de manifiesto la realidad de la delincuencia informática en contraste con el marco penal establecido, verificando los problemas que encuentra la actual regulación en su aplicación por los operadores del Derecho y por las Fuerza y Cuerpos de Seguridad del Estado, y las soluciones que pueden tratar de mitigar estos efectos negativos de la regulación. El capítulo quinto concluye con la proposición de un nuevo marco penal para los delitos de daños informáticos y otras acciones conexas. Esta propuesta, si bien se encuentra incardinada en el último capítulo, trata de responder a los problemas que se hayan ido suscitando a lo largo de la investigación, de forma que pueda llegar a constituir una referencia para el legislador en el futuro.

Por último, no queremos cerrar esta introducción sin advertir al lector de que con la elaboración del presente trabajo nos han ido asaltando diferentes problemas de terminología utilizada en los tipos penales que ahora vamos a analizar. “El lenguaje

es el vestido del pensamiento"[23] y por lo tanto, si se quiere tener un pensamiento inequívoco y común, es necesario utilizar un lenguaje igualmente inequívoco y común; palabras que adquieren todavía mayor significado cuando nos situamos en la esfera del Derecho penal, en el cual la literalidad y taxatividad de los preceptos funciona como un principio rector, y más ahora, ya que en las cuestiones que nos ocupan, muchas veces, resulta complicado trazar la línea divisoria entre el concepto común de una palabra y su significado técnico informático. Añadido a esto, lamentablemente, no existe un diccionario de términos informáticos, o mejor expresado, existen tantos como podamos imaginar, lo que produce que en muchos casos sea necesario acudir primero a la reflexión sobre lo que entendemos por uno u otro concepto para luego poder realizar un análisis jurídico adecuado que permita encajar dicho concepto en los textos legales oportunos. Aunque se intentará ofrecerr a lo largo de las páginas que siguen, siempre que sea oportuna, la información básica para entender en su plenitud cada concepto que tratemos, lo cierto es que no siempre existe unidad de criterio para determinar con exactitud el alcance y contenido de algunas palabras[24].

Por ello, hemos querido dedicar el capítulo primero a estos problemas. Creemos que la envergadura y problemática que suscita la materia objeto del presente trabajo de investigación excede los límites estrictamente jurídico-dogmáticos del mismo, por lo que vamos a otorgar el suficiente desarrollo a otras cuestiones importantes que se encuentran inexorablemente conectadas con la figura de los daños informáticos. En primer lugar, parece que es oportuno realizar una introducción histórica dedicada a la informática que nos permita valorar la complejidad de la ciencia ante la que nos encontramos. Junto a esta aproximación histórica analizaremos desde un punto de vista general, pero suficientemente amplio, los comportamientos informáticos que podemos denominar abusivos o reprochables socialmente, de forma que conozcamos adecuadamente la peor de las caras de la informática

[23] Cita atribuida a SAMUEL JOHNSON (Lichfield, Staffordshire, 18 de septiembre de 1709 - Londres, 13 de diciembre de 1784).

[24] En la Red existen multitud de páginas web con definiciones más o menos acertadas, por ello conviene siempre acudir a más de una de ellas para contrastar la información encontrada o, en general, conseguir diccionarios editados y publicados por editoriales con reconocimiento internacional.

Este primer capítulo ha sido el último en ser elaborado, pues aun no siendo, como se comprenderá, el tema central de la investigación, no se puede dejar de guiar convenientemente al lector dentro de unos márgenes que sin lugar a dudas se hace imprescindible exponer para la total comprensión de la problemática a la que nos enfrentamos. Con la intención de no alejarnos en exceso de la temática jurídica, a lo largo del mismo, iremos dando las primeras pinceladas vinculadas con su repercusión posterior en el análisis de las figuras penales. Por eso, su lectura, más allá de suponer una fuente de información útil para cualquier interesado tanto desde una perspectiva jurídica como ajena al mundo del Derecho es, a nuestro juicio, fundamental para comprender en su plenitud el resto de la investigación.

Como hemos señalado, la aparición de Internet y el llamado ciberespacio se ha convertido, a la vez que en una herramienta fundamental, en el origen de un cúmulo de situaciones que requieren nuevas soluciones desde la perspectiva jurídica, ya sea en el ámbito penal que a continuación va a ser tratado, como en el administrativo, civil, mercantil e incluso constitucional[25].

[25] TEUBNER, G.: "Globalización y constitucionalismo social: alternativas a la teoría constitucional centrada en el Estado" en BACIGALUPO SAGGESE, S. y CANCIO MELIÁ, M. (coords.): *Derecho penal y política transnacional*, Ed. Atelier, 1ª edición, Barcelona, 2005, pp. 19 y ss.

PRIMERA PARTE:

LA INFORMÁTICA Y LA DELINCUENCIA INFORMÁTICA EN ESPAÑA Y EN EL MUNDO

CAPÍTULO PRIMERO: LA INFORMÁTICA Y LOS ABUSOS COMETIDOS A TRAVÉS DE SISTEMAS INFORMÁTICOS

1. INTRODUCCIÓN

El presente trabajo de investigación centra su desarrollo en el ámbito jurídico-penal de determinadas acciones cometidas contra sistemas informáticos. Parece adecuado, sin embargo, comenzar el mismo con una breve pero importante introducción sobre la ciencia en la que se originan las conductas que más tarde van a ser estudiadas.

Es sabido que el Derecho, como elemento regulador de las relaciones sociales, no puede prever en su totalidad los caminos que éstas siguen en el desarrollo de los diversos modelos de evolución. El caso de los delitos informáticos en general, que podríamos denominar como aquellos cometidos contra, o a través, de medios informáticos, no escapa a esta lógica, que se ha visto además agravada por el avance vertiginoso de la informática y las telecomunicaciones[26].

En las próximas líneas, dejando por el momento de lado el mundo del Derecho, vamos a realizar un breve análisis histórico en cuanto a lo que a la informática se refiere. Veremos que a partir de la primera mitad del siglo XX la evolución de la técnica informática sufre un marcado aumento de velocidad en su desarrollo práctico, y que a finales de ese mismo siglo XX el panorama es prácticamente irreconocible, habiéndose creado una dependencia casi inseparable entre la vida normal en la sociedad y la interacción del hombre con las máquinas. De está interacción surgen nuevas conductas humanas cuya regulación se hace necesaria, momento en el cual el Derecho debe proponer la soluciones más adecuadas. En un sentido negativo, también aparecen usos reprochables y abusos por parte de nuevos sujetos con conocimientos, no necesariamente avanzados, sobre la utilización de

[26] Señala acertadamente LAGARES GARCÍA, D.: *Internet…* ob. cit. p. 34, que "la fuerte evolución de las tecnologías y su veloz instauración en nuestras vidas, como algo común e indispensable, ha puesto en evidencia la lentitud con la que la Ciencia Jurídica responde tras realizarse el cambio sociológico".

estos nuevos sistemas[27]; siendo entonces necesaria también la regulación penal de ciertos aspectos de la informática[28].

A estás cuestiones introductorias relativas a la historia de la informática, la terminología actual, y las prácticas abusivas que se realizan a través de los sistemas informáticos dedicaremos este primer capítulo.

2. INFORMÁTICA BÁSICA. ORIGEN Y EVOLUCIÓN

La informática, entendida como ciencia, aparece en un momento relativamente moderno de la historia, si bien mucho anterior a lo que imaginamos[29] y en todo caso en un momento histórico muy anterior al del nacimiento del Derecho de la informática que, por tanto, se ve obligado a integrarla en sí mismo. Para ello crea nuevas instituciones, y dota de un carácter jurídico a ciertos elementos propios de la informática y las telecomunicaciones.

Estás primeras páginas acercan al lector a la informática desde un prisma sustancialmente ajeno al Derecho para, a continuación, ir poco a poco engarzando con la temática propia del resto del texto, esto es, con el tratamiento penal que se hace de ciertas acciones cuyo razón de ser se encuentra en la informática. Porque la informática, como fenómeno social, no debe escapar a unas reglas que la regulen y la limiten, y en muchos casos, no debe suponer excusa para no castigar a ciertos sujetos que utilizan sus conocimientos sobre la misma para llevar a cabo acciones reprochables, y que, en consecuencia, deben encontrar acomodo en las ramas clásicas del Derecho, en nuestro caso, el Derecho penal, para así conseguir una adecuada

[27] Aunque será tratado desde diversos puntos de vista más adelante, el delincuente informático no tiene que ser necesariamente un experto en informática, puede ser simplemente un usuario con conocimientos básicos o, según el tipo de regulación de la que estemos hablando, un lego en la materia que causa un daño informático sin para ello utilizar siquiera medios informáticos.

[28] Si bien será tratado más adelante, podemos señalar ahora que tras la aparición de los primeros virus informáticos dañinos en 1986 surgieron las primeras regulaciones penales al respecto en Estados Unidos y algunos países de Europa.

[29] Para una visión histórica ordenada por personajes relevantes DAVIS, M.: *Universal computer. The road from Leibniz to Turing*, Ed. W.W. Norton & Company, 1ª edición, Nueva York, 2000. Aunque el creador de la primera máquina programable de la historia suele asociarse con Konrad Zuse (1910-1995), fue G.W. Leibniz (1646-1716) el primero en plantear la importancia de la mecanización del cálculo. También la página web http://www.computerhistory.org

protección del ciudadano, lo que repercutirá indudablemente en la idea de construir una sociedad mejor.

A) EL ORIGEN DE LA INFORMÁTICA

La informática moderna es el resultado de una serie de investigaciones y descubrimientos llevados a cabo por un numeroso elenco de personajes históricos, cada uno de los cuales ha contribuido, en parte, a una evolución constante hasta conseguir el nivel de desarrollo tecnológico actual[30]. Cabría destacar, en primer lugar, que el origen de la informática era conseguir la mecanización de cálculos matemáticos, de tal forma que se pudiesen llevar a cabo gran número de cálculos con poco esfuerzo humano[31]. De ello se puede extraer sencillamente que la informática está basada, principalmente, en cuanto a su plano teórico se refiere, en las matemáticas[32].

De hecho, la primera persona que entendió la utilidad de la mecanización del cálculo era, en todos los sentidos, un matemático, G.W. Leibniz (1646-1716). Y si su labor como matemático no se diferenció específicamente de la de sus predecesores, si lo fue la idea que estableció de mejorar el cálculo a través de la utilización de máquinas[33], idea sobre la cual empezaron a volcarse en lo sucesivo otros físicos y matemáticos, produciéndose en los dos siguientes siglos los primeros avances relevantes en la mecanización del cálculo.

Continuando con la idea de utilizar máquinas para realizar cálculos, resulta fundamental la máquina analítica del matemático Charles Babbage (1791-1871), que se configuraba como un ordenador de uso general programable y no sólo una

[30] Una visión muy general de sujetos y sucesos interesantes sobre la era de la informática se puede ver en GRAHAM, P.: *Hackers & painters*, Ed. Sebastopol, 1ª edición, California, 2004.

[31] DAVIS, M.: *Universal*… ob. cit. pp. 8 y ss.

[32] GOLDSTINE, H.H.: *The Computer, from Pascal to Von Neumann*, Ed. Princeton University Press, 5ª edición, Nueva Jersey, 1993, pp. 3-9, señala la importancia de algunos personajes históricos en el campo de las matemáticas y el álgebra como Galileo (1564-1642), René Descartes (1596-1650) o Pascal (1623-1662) para el desarrollo posterior de la informática.

[33] DAVIS, M.: *Universal*… ob. cit. p. 8. También fue el precursor del sistema binario, en el que está basado el funcionamiento actual de los ordenadores modernos. Para un análisis más extenso de la figura se recomienda EBERHARD, J.A. y ECKHART, J.G.: *Leibniz-Biographien*, Ed. Olms, 2ª edición, Hildesheim, 2003.

computadora aritmética. Su máquina analítica nunca llegó a ser construida, entre otras cuestiones por las dificultades técnicas que suponía hacerlo en esa época[34]. En 1936 Alan Turing describe la máquina de Turing basándose en los trabajos de Babbage. Al contrario de las pretensiones de su predecesor, el modelo de Turing era un modelo esencialmente teórico, y su objetivo no se centraba en construir un ingenio mecánico que cumpliese con la teoría por él expuesta. Sin embargo la relevancia científica de su teoría se fundamenta en que los ordenadores construidos con posterioridad responden perfectamente al modelo de la máquina de Turing[35].

Se concluye, en todo caso, que la informática como tal no se puede vincular fácilmente con un solo hombre, sino que se configura como el resultado evolutivo e integrador de las matemáticas, pero también de la física de los materiales, el álgebra, la lógica y muchas otras ciencias teóricas que dan como resultado la ciencia aplicada que hoy se conoce como informática.

B) LA INFORMÁTICA MODERNA

En general existe común aceptación por parte de los expertos en fijar el inicio de la informática práctica con la aparición del sistema Z3[36] creado por Konrad Zuse (1910-1995) en 1941[37]. Este sistema informático fue el primero en ser programable y

[34] DAVIS, M.: *Universal…* ob. cit. pp. 139 y 140. Para un análisis más extenso de la figura se recomienda HYMAN, A.: *Charles Babbage: pioneer of the computer*, Ed. Princeton University Press, 1ª edición, Nueva Jersey, 1985.

[35] DAVIS, M.: *Universal…* ob. cit. pp. 163-167 y O'REGAN, G.: *A brief history of computing*, Ed. Springer, 1ª edición, Londres, 2010, pp. 48-50. Para un estudio más detallado de la figura se recomienda PETZOLD, C.: *The annotated Turing: a guided tour through Alan Turing's historic paper on computability and the Turing machine*, Ed. Wiley Pub, 1ª edición, Indianapolis, 2008.

[36] El Z3, de tecnología electromecánica, estaba construido con 2300 relés, tenía una frecuencia de reloj de 5 Hz, y una longitud de palabra de 22 bits. Los cálculos eran realizados con aritmética en coma flotante puramente binaria. El Z3 original fue destruido en 1943 durante un bombardeo aliado de Berlín. Una réplica completamente funcional fue construida durante los años 60. En 1998 se demostró que el Z3 es una máquina de Turing completa. Véase la web del departamento de matemática aplicada de la Universidad Politécnica de Madrid:
http://www.eui.upm.es/escuela/dptos/ma

[37] Es curioso que, sin embargo, este hecho no fuese descubierto hasta después de la Segunda Guerra Mundial, pues la fabricación del Z3 se llevó a cabo en la Alemania Nazi, y los descubrimientos de Zuse no pudieron ser conocidos por sus colegas americanos hasta una vez terminada la guerra. O'REGAN, G.: *A brief…* ob. cit. pp. 69 y 70. No se le puede considerar en todo caso el inventor de la informática, pues ya se ha señalado que existen propuestas teóricas anteriores

totalmente automático. Aunque su tamaño y forma de construcción dista mucho de los procesos de creación de sistemas informáticos actuales, su modo de funcionamiento desde una perspectiva puramente informática es básicamente igual al de los ordenadores modernos.

A partir de este momento se considera que comienza la historia de la informática moderna, cuyos logros más importantes sólo cabe ahora señalar, pero que como es lógico nos llevan hasta nuestros días. Quizá la nota característica de todos los avances posteriores a la creación del Z3 se centran en cuestiones relativas a la miniaturización de los sistemas, el aumento de su capacidad de procesos por unidad de tiempo a través del desarrollo de la electrónica y la integración de sistemas de apoyo anexos a la propia computadora para, en un momento algo más avanzado, dar comienzo a la creación de las redes informáticas.

El ENIAC[38] creado en 1946 era capaz de realizar cinco mil operaciones aritméticas por segundo, su tamaño era el equivalente a varios campos de futbol y su consumo eléctrico estratosférico[39]. En 1949 se crea la primera "memoria" que sustituye a los tubos de vacío como elemento para almacenar datos. En la década de 1950 comienzan a desarrollarse lenguajes de programación más eficientes[40] junto con nuevos ordenadores capaces de realizar mayor número de procesos por unidad de tiempo gracias a la concepción de nuevas técnicas para su construcción[41].

En la actualidad la estructura de los ordenadores es semejante a la establecida en las máquinas de los años 60, si bien la capacidad de proceso ha aumentado

---

cuyo resultado era similar, pero cuya demostración empírica de validez no se puedo llevar a cabo hasta un momento posterior. Por ello, si es cierto que se debe reconocer a Konrad Zuse como creador del primer sistema informático moderno, no así se puede considerar como el creador de la informática moderna desde un plano teórico que corresponde al ya mencionado Charles Babbage (1791-1871) considerado "El padre de la computación". DAVIS, M.: *Universal*… ob. cit. p. 165 y ss. y O'REGAN, G.: *A brief*... ob. cit. p. 36.

[38] Siglas en inglés de *Electronic Numerical Integratos and Calculator.*

[39] GOLDSTINE, H.H.: *The Computer*... ob. cit. pp. 157 y ss.

[40] GOLDSTINE, H.H.: *The Computer*… ob. cit. pp. 333 y ss. y O'REGAN, G.: *A brief*... ob. cit. pp. 76 y 77.

[41] En esta labor se antoja fundamental el papel de la compañía americana IBM, fundada en 1911 y conocida como tal a partir de 1924, CAMPBELL-KELLY, M. y ASPRAY, W.: *Computer: a history of the information machine*, Ed. Westview Press, 2ª edición, Boulder, 2004, pp. 117 y ss.

significativamente gracias, en parte, a la utilización de nuevos materiales para la construcción de los componentes y la miniaturización de estos. Cuestiones todas ellas que han producido que la implantación en la sociedad de tales máquinas haya alcanzado un nivel inimaginable hace tan solo unas décadas[42].

Cabe por ahora señalar que durante los primeros pasos de la informática moderna no aparece (tampoco anteriormente) en la sociedad la necesidad de una regulación específica en el ordenamiento jurídico en este ámbito. Principalmente se trataba de investigaciones privadas con escasa trascendencia pública, o bien de proyectos de universidades o administraciones públicas, si bien es cierto que ya se comenzaban a vislumbrar las posibilidades en negativo de los avances técnicos de la mecanización de cálculos en el campo militar para la decodificación de mensajes cifrados[43]. En la década de 1940 eran ya conocidos los denominados *bugs* o fallos de seguridad en los sistemas que podían producir un mal funcionamiento del mismo[44]. Sin embargo la existencia de estos fallos de seguridad no supondría un problema relevante que necesitase la intervención del ordenamiento jurídico sino hasta la década de 1970 y, en adelante, con la aparición y estandarización de las redes de ordenadores y los ordenadores personales.

b.1. La aparición de los ordenadores personales.

A partir de la década de 1970, a lo largo de la evolución antes descrita, se produce una inflexión con la invención del microprocesador, gracias a la cual se

[42] Sobre este aspecto se recomienda la lectura completa del capítulo 10 (pp. 207-230) de CAMPBELL-KELLY, M. y ASPRAY, W.: *Computer*… ob. cit.

[43] Durante los años 30 y 40 se normaliza la utilización de los ordenadores para estos fines militares. Se recomienda SMITH, M.: *Station X: The Codebreakers of Bletchley Park, Pan Grand Strategy Series*, Ed. Pan mcmillan Ltd, 1ª edición revisada, Londres, 2007 y WELCHMAN, G.: *The Hut Six story: Breaking the Enigma codes*, Ed. Penguin Books, 1ª edición revisada, Harmondsworth, 1984, pp. 70 y ss.

[44] Aunque Thomas Edison ya señalaba en sus obras científicas los fallos en sistemas eléctricos con la denominación *bug*, se comenzó a utilizar esta misma palabra para los fallos en los ordenadores a partir de la década de 1940, especialmente a partir del fallo provocado por un insecto (en inglés *bug*) en un ordenador de la época. *National Museum of American History* (http://americanhistory.si.edu/collections) objeto 1994.0191.01, se puede leer: "Primera causa del fallo del sistema encontrada: Un polilla [*bug* en inglés] en un relé. Primera vez que se encuentra en un ordenador un *bug* de verdad."

consiguen abaratar significativamente los costes de producción de los ordenadores y, no menos importante, el tamaño de éstos. La computadora personal se orientaba al individuo, y aunque las primeras máquinas requerían de un conocimiento al menos avanzado del usuario final, ya se percibía la necesidad de dotar a las mismas de un sistema de funcionamiento sencillo[45]. En 1971 se presenta el primer microprocesador con carácter comercial[46] y también en 1971 es creado el primer virus informático, aunque sobre ello nos detendremos más adelante

A nivel empresarial, cabe destacar la aparición de Intel en la década de 1960, y la de Apple y Microsoft en la de 1970. En general comenzará a recaer sobre un selecto grupo de compañías el desarrollo de la informática a partir de la década de 1980[47] coincidiendo en el tiempo con el principio de la era de la informática personal y el nacimiento de Internet[48]. Con ello comienza la carrera comercial por llevar a cada hogar un ordenador, idea que continua siendo el motor del desarrollo de la informática comercial hoy en día, aunque ligado a la aparición de nuevos dispositivos portátiles, y la integración de la telefonía, fotografía, etc. en un único sistema informático.

Aunque este estudio centra todo su desarrollo en el análisis de jurídico de las acciones cometidas contra sistemas informáticos cuyo origen se encuentra en la máquina Z3 de Konrad Zuse (básicamente ordenadores que utilizan el código binario clásico), a partir de la década de 1980 se empieza a desarrollar la informática cuántica[49], cuyo funcionamiento y principios son considerablemente diferentes a los

[45] CERUZZI, P.E.: *A History of Modern Computing*, Ed. MIT Press, 2ª edición, Cambridge, 2003, pp. 177 y ss.

[46] CAMPBELL-KELLY, M. y ASPRAY, W.: *Computer…* ob. cit. pp. 209 y ss.

[47] A las ya nombrada IBM, Intel, Apple y Microsoft se sumarán Sony, Compaq, HP, etc. Y en un pasado reciente todas las compañías surgidas como consecuencia de la explosión de Internet como Yahoo! o Google.

[48] CERUZZI, P.E.: *A History…* ob. cit. pp. 207 y ss.

[49] La Universidad de Oxford cuenta con el *Centre for Quantum Computation* (http://www.qubit.org). De reconocido prestigio es igualmente el IQC (siglas en inglés de *Institute for Quantum Computing*), el Instituto de la Universidad de Waterloo dedicado a la investigación del universo cuántico para la transformación de la informática y las telecomunicaciones (http://iqc.uwaterloo.ca). En España uno de los grupos de trabajo más importantes es el Grupo de Investigación en Información y Computación Cuántica de la Universidad Politécnica de Madrid (http://gcc.ls.fi.upm.es).

de la informática moderna[50]. Aunque el ordenamiento jurídico no ha entrado en la regulación de nuevas situaciones debido al escaso desarrollo de está tecnología, cabe destacar que la estandarización de normas adecuadas para la regulación de determinados usos de la informática moderna no se acaba con su aprobación, sino que debido a la naturaleza del campo que intenta regular, su revisión debe ser una constante para mantener un sistema normativo adecuado a un mundo que, como sabemos, cambia constantemente.

b.2. La aparición de las redes informáticas.

A la explosión del avance informático de mediados del siglo XX aparece ligada la idea de no concebir los ordenadores como meros instrumentos singulares, sino interconectar dos o más de ellos de forma que puedan compartir la información (los cálculos) unos con otros, aumentar la capacidad de trabajo dividiendo tareas, y conseguir mayor seguridad distribuyendo los riesgos de perder información producto de averías o fallos (o ataques) de los sistemas individuales.

A partir de esta idea en 1969 se crea la primera red de computadoras, ARPANET[51], desarrollada por el Departamento de Defensa de los Estados Unidos de América, germen de Internet[52]. ARPANET fue la red base de Internet hasta 1990. El primer punto de acceso se creó en la Universidad de California en Los Ángeles. Inicialmente se proyectaron cuatro puntos de acceso: además de dos ordenadores en la Universidad de California; los otros ordenadores de la red se localizaban en el ARC[53] en el Instituto de Investigación de Stanford y en el Departamento Gráfico de la Universidad de Utah. La primera conexión de ARPANET se estableció el 21 de noviembre de 1969 entre la Universidad de California y Stanford. El 5 de diciembre

[50] Para un conocimiento básico consultar RAYO, A.: "Computación cuántica" en *Investigación y Ciencia*, nº 405, 2010, pp. 92 y 93. Para un conocimiento avanzado NIELSEN, M. A. y CHUANG, I. L.: *Quantum Computation and Quantum Information*, Ed. Cambridge University Press, 10ª edición, 2011.

[51] Siglas en ingles de *Advanced Research Projects Agency Network*.

[52] ABBATE, J.: *Inventing the Internet*, Ed. MIT Press, 1ª edición, Cambridge, 1999, pp. 36 y ss. Para un conocimiento técnico se recomienda BANKS, M. A.: *On The way to the web: the secret history of the internet and its founders*, Ed. Springer-Verlag, 1ª edición, Nueva York, 2008.

[53] Siglas en ingles de *Augmentation Research Center*.

del mismo año toda la red inicial estaba lista[54]. En los siguientes años se realizaron las primeras conexiones transoceánicas con Noruega y Reino Unido y se estableció un protocolo común para la comunicación de sistemas informáticos diferentes[55]. En 1985 Internet ya era una tecnología totalmente establecida, aunque desconocida para la mayor parte de la población por la escasa implantación de los ordenadores personales. En 1990 se estima que existían alrededor de 100.000 ordenadores conectados. En esa misma época se concluye que el modelo de búsqueda de ordenadores en la red comienza a resultar caótico debido al número de terminales conectados, por ello investigadores del CERN[56] crean el protocolo de nombres WWW[57] que ve la luz en 1992.

Es en ese momento, aproximadamente coincidente en el tiempo con el comienzo de la masificación del ordenador personal, cuanto Internet comienza a crecer más rápido que cualquier otro medio de comunicación, convirtiéndose en lo que hoy todos conocemos[58].

---

[54] O'REGAN, G.: *A brief…* ob. cit. pp. 179 y ss.

[55] El protocolo de comunicación TCP (siglas de *Transmission Control Protocol*) es fundamental todavía hoy en día para entender el funcionamiento de Internet. Su función principal radica en realizar las conexiones entre los ordenadores, de tal forma que se pueda producir el envío de datos entre ellos. Es decir, su función principal es que dos ordenadores se entiendan cuando establecen comunicación, es el idioma principal de las comunicaciones entre ordenadores; en O'REGAN, G.: *A brief…* ob. cit. pp. 183 y 184.

[56] Siglas en francés de *Conseil Européen pour la Recherche Nucléaire.*

[57] Siglas en ingles de *World Wide Web*. Este nuevo modelo permitía vincular información en forma lógica a través de las redes. El contenido se programaba en un lenguaje de hipertexto de forma que se le asignaba una función para luego, gracias a un programa que ejercía de intérprete y era capaz de leer el hipertexto y mostraba la información que el usuario deseaba. Nacen así los navegadores de Internet. En 1993 aparece públicamente la primera versión del navegador Mosaic, pionero y que permitió acceder con mayor facilidad a los contenidos alojados en Internet. Rápidamente se descubrió la utilidad de contar con una interfaz gráfica y la facilidad con la que se podía manejar el programa incluso para aquellos con pocos conocimientos de informática. Mosaic fue finalmente superado en 1994 por Netscape Navigator como el navegador web más popular en el mundo. Aparecieron entonces los navegadores de Internet que sustancialmente ahora conocemos (Internet Explorer, Opera, Mozilla Firefox, etc.). O'REGAN, G.: *A brief…* ob. cit. pp. 185 y ss.

[58] El crecimiento exponencial de la web provocó la creación de directorios web en primer lugar, y de buscadores más adelante. Su función era localizar las páginas web en la red de tal forma que se facilitase a los usuarios encontrar la información que buscaban en el cada vez mayor océano de información que se abría paso. Los primeros buscadores fueron Lycos en 1993 (éste, además, llegó a obtener cierto éxito internacional) y Web Crawler en 1994. Yahoo! y Altavista fueron fundados en 1995 en el momento en que Internet comenzaba a llegar a gran cantidad de hogares en Estados

Hoy en día Internet llega en España a 23 millones de usuarios, esto es la mitad de la población del país, con una marcada tendencia positiva en la tasa de penetración. Además, de esos usuarios, el 90% accede a la red desde sus hogares, lo que se traduce en una implantación casi total del ordenador (o equivalente) y de Internet en el hogar español. En el mundo se estima que más de 2.000 millones de personas acceden a Internet, un 30% de la población mundial.[59]

Estos datos muestran la importancia del estudio jurídico-penal que nos disponemos a realizar. Se puede afirmar que en España la normalización del uso de los ordenadores y de Internet es una realidad, y por tanto no podemos negar la necesidad de tener un marco jurídico adecuado a esta situación. La mitad de la población utiliza Internet, y podemos presumir que un número superior utiliza ordenadores personales u otros dispositivos electrónicos análogos, lo que multiplica las posibilidades de que sobre dichos dispositivos se produzcan hechos socialmente reprochables que, de no tener una adecuada respuesta por parte del ordenamiento jurídico, provocarían una significativa alarma social. Y todo ello se ve incrementado exponencialmente por la transnacionalidad de las redes informáticas. La interconexión de ordenadores de todo el mundo significa un aumento de las posibilidades de aparición de acciones negativas desde y hacía los sistemas de los usuarios de dispositivos informáticos en España, y su persecución adquiere una mayor complejidad[60].

Unidos, Japón y Europa. El último buscador de relevancia comercial es el desarrollado por la compañía Google que vio la luz en 2001, pronto se convertiría en el buscador de referencia gracias al desarrollo del ordenamiento de resultados por relevancia. O'REGAN, G.: *A brief*... ob. cit. pp. 188 y ss. También REYNA ALFARO, L. M.: "La criminalidad informática: cuestiones para una reflexión inicial" en *Actualidad Penal*, nº 21, 2002, pp. 528 y ss.

[59] Datos del informe *La situación de Internet en España y en el Mundo en 2012*. Estudio más reciente de carácter privado realizado por la consultora española Tatum.

[60] DÍAZ GÓMEZ, A.: "El delito…" ob. cit. pp. 173 y 174, señala acertadamente que "la inexistencia de fronteras reales es una de las características intrínsecas de Internet, que ofrece innumerables ventajas y como no podía ser de otro modo, inconvenientes para la persecución de actividades delictivas. En primer lugar, para iniciar cualquier política criminal, hay que conocer cuál va ser el terreno de actuación. Dicho de otra manera, saber «dónde está Internet»; estamos ante uno de los grandes problemas que existen, dada la dificultad de responder con exactitud a dicha pregunta […] Pero además, y dado que a la Red se puede acceder desde cualquier parte del mundo prácticamente al instante, el siguiente problema relacionado con la independencia geográfica de Internet lo encontramos en la dificultad de perseguir un ilícito de estas características. Quiérase decir que un

Además de ello, Internet hoy en día no se utiliza simplemente para conseguir información por parte de los usuarios, sino que es una auténtica herramienta de interacción social (relaciones personales, trabajo o comercio, por poner algunos ejemplos), utilizada por empresas, consumidores, estudiantes, administraciones públicas, etc[61]. Lo que incide en la necesidad de tutelar el correcto funcionamiento de la red, en cuanto a la protección -sin entrar ahora en un debate técnico jurídico extenso- del orden público, el patrimonio y la libertad de las personas.

C) TERMINOLOGÍA EN LAS ACTIVIDADES INFORMÁTICAS

Como señalábamos al inicio de este capítulo, esta breve introducción responde al interés de fijar desde el principio una serie de pautas generales sobre la terminología concreta en el ámbito de la informática, para tras ella realizar el análisis jurídico de la regulación de los delitos de daños informáticos recogidos en el artículo 264 CP.

Si bien en las páginas anteriores ya hemos referido determinados vocablos que se ubican específicamente en el campo de la informática, también existen ocasiones en las que esas mismas palabras se utilizan en un ámbito coloquial de forma no del todo adecuada. No es exactamente lo mismo un ordenador que un sistema informático, ni una red informática que Internet, o por mencionar conceptos que ha utilizado el legislador español, no son lo mismo datos informáticos, programas informáticos o documentos electrónicos[62].

---

sujeto puede cometer un delito contra otro situado a miles de kilómetros del primero, mientras que la información está en otro lugar diferente de éstos. La situación puede llegar a producir una verdadera impunidad, si no se articulan los remedios adecuados".

[61] DÍAZ GÓMEZ, A.: "El delito…" ob. cit. p.171, señala que "si algo ha revolucionado la sociedad es Internet, gran invento del siglo XX y símbolo de la época actual. Internet ha facilitado las relaciones sociales, y en general toda comunicación e intercambio de información. Pero aún más; ha alterado de manera decisiva e irreversible nuestro modo de vivir y acercarnos a los demás".

[62] Del tenor literal del artículo 264 CP podría deducirse que son conceptos análogos o semejantes, y aunque en términos coloquiales pueden serlo, estrictamente hablando son cosas diferentes, que quizá no merezcan esa equiparación por parte del legislador. En el capítulo tercero de la investigación, al estudiar el objeto material del delito, nos detendremos convenientemente en el análisis de las diferencias entre los mismos.

En el ámbito del Derecho penal el principio de legalidad[63] rige imperativamente consagrando la máxima *nullum crime, nulla poena sine lege*, la cual en su desarrollo, viene a devenir en una serie de garantías[64] y exigencias[65] como consecuencia de las cuales se hace inexcusablemente necesario un uso concreto de los conceptos, con un significado, en la medida de lo posible, con vocación de permanencia y determinación objetiva[66]. Actuar de forma contraria y no seguir este principio podría provocar, entre otras, la poco recomendable situación de interpretar de forma diferente los conceptos en cada momento determinado, lo que nos conducirá irremediablemente a una falta de seguridad jurídica a la hora de analizar conceptos informáticos desde la perspectiva del Derecho penal. En los ejemplos expresados anteriormente, es importante conocer el concreto significado con el que el legislador ha querido dotar a cada palabra. En la utilización de los conceptos adecuados a la hora de redactar los textos de la norma penal radica el elemento fundamental de la misma, es decir, su aplicabilidad. Un concepto ambiguo o general podría llevar a una sobreprotección penal inadecuada, al mismo tiempo una concreción excesiva en la regulación podría dejar fuera, tras una aplicación de la ley según el elemento gramatical de la misma, conductas reprochables cuyo objetivo inicial con la regulación era la prohibición[67].

[63] El Principio de legalidad se encuentra recogido tanto en la Constitución española en su artículo 25, como en el Código penal, concretamente en los artículos 1, 2 y 3.

[64] MIR PUIG, S.: *Derecho Penal. Parte General*, Ed. Reppertor, 8ª edición, Barcelona, 2010, p. 106, señala como tales garantías: la criminal (exigencia de que el delito se encuentre en una ley), la penal (que además se señale la pena que acompaña al delito en la ley), la jurisdiccional (imposición a través de una sentencia judicial después de un proceso establecido) y la de ejecución (que la ejecución de la pena también esté sujeta a una ley que la regule). También HUERTA TOCILDO, S.: "Principio de legalidad y normas sancionadoras" en *El principio de legalidad. Actas de las V Jornadas de la Asociación de Letrados del Tribunal Constitucional*, Ed. Centro de Estudios Políticos y Constitucionales, 1ª edición, Madrid, 2000, pp. 16 y ss.

[65] Estas exigencias serían *lex praevia, lex scripta* y *lex stricta.* STC 133/1987, de 21 de julio, F. 4. Continuadoras de esta doctrina son también las SSTC 111/1993, de 25 de marzo, F. 6; 372/1993, de 13 de diciembre, F. 5; y 64/2001, de 17 de marzo, F. 4. También el TS más recientemente siguiendo esta doctrina STS 1387/2011, de 12 diciembre, F. 11.

[66] Sobre el lenguaje en las leyes ver GARCÍA-ESCUDERO MÁRQUEZ, P.: *Manual de técnica legislativa*, Ed. Civitas, 1ª edición, Madrid, 2011, pp. 150 y ss.

[67] QUINTERO OLIVARES, G.: *Parte General del Derecho Penal,* Ed. Thomson Reuters, 4ª edición, Navarra, 2010, pp. 130 y ss., sostiene que el elemento gramatical es el más adecuado para interpretar la ley penal, primero en importancia frente al elemento histórico, lógico, sistemático o teleológico. En

A continuación se exponen los conceptos ordenados para su mejor compresión, partiendo del concepto general de ordenador. Cabe destacar que en muchos casos la RAE no realiza una definición de los términos explicados, o en su caso, ofrece un concepto que no cubre totalmente un significado adecuado del vocablo en cuestión. Por ello, la única manera de abarcar completamente el significado de cada palabra es acudir a las definiciones que se otorgan por los propios expertos en diferentes medios y aplicarlo a nuestro caso concreto[68]. Aunque cuando llegue la hora de analizar la estructura, alcance y significado de los concretos tipos penales de daños informáticos volveremos sobre la interpretación que se debe hacer de ciertas palabras, la finalidad de este capítulo introductorio es fijar un marco general sobre el cual poder desarrollar convenientemente las demás partes de la investigación.

c.1. Ordenador, sistema informático y redes de sistemas informáticos.

Para la RAE ordenador es una "máquina electrónica dotada de una memoria de gran capacidad y de métodos de tratamiento de la información, capaz de resolver problemas aritméticos y lógicos gracias a la utilización automática de programas registrados en ella". En la misma línea define una computadora como una "máquina electrónica, analógica o digital, dotada de una memoria de gran capacidad y de métodos de tratamiento de la información, capaz de resolver problemas matemáticos y lógicos mediante la utilización automática de programas informáticos". De esto se puede extraer que en la actualidad son palabras sinónimas, siendo la más utilizada en España la palabra ordenador (del francés *ordinateur*), mientras que en Latinoamérica es la palabra computadora (del inglés *computer*) la de mayor uso.

Para poder hablar entonces de un ordenador en pleno funcionamiento se hace necesaria la conjunción de un *hardware* (dispositivo físico) y un *software* (dispositivo lógico o inmaterial) operativos de tal forma que el ordenador pueda ejecutar a través del *software* las funciones para las que está preparado el *hardware*.

---

este sentido es igualmente inasumible la utilización de la analogía para introducir supuestos reprochables que han quedado excluidos por una deficiente técnica legislativa.

[68] Ante la falta de una concreción exacta a menudo los autores de manuales, artículos o páginas webs, y expertos en general, realizan definiciones de conceptos informáticos generales adaptadas a los temas concretos del campo particular que van a tratar.

c.1.1. Conceptos en torno a la idea de hardware.

La RAE se limita a señalar que *hardware* es el "conjunto de los componentes que integran la parte material de una computadora", lo que es una definición claramente insuficiente, en el sentido de ser demasiado general.

Una definición más adecuada para los propósitos generales de este estudio es la que entiende por *hardware* las partes tangibles o físicas de un sistema informático; normalmente compuestas por sistemas eléctricos, electrónicos y mecánicos[69]. Esto es así porque en primer lugar, no limita la definición a los componentes de un ordenador, como si hace la RAE, sino que se refiere a cualquier sistema informático que, ahora explicaremos, es un conjunto más amplio. Además, de la definición de la RAE parece desprenderse que nos referimos a componentes físicos internos del ordenador, lo cual tampoco es correcto. Así, los denominados periféricos de un ordenador o de un sistema informático en general también deben ser considerados *hardware* (monitores, impresoras, memorias externas, etc.); y no sólo ello, sino que algunos de estos periféricos pueden suponer sistemas informáticos en sí mismos, es decir, en función del momento concreto pueden funcionar bien como periféricos o bien como sistemas informáticos autónomos[70]. Respecto a esta idea es necesario, por tanto, hacer una distinción básica entre *hardware* básico de un sistema y *hardware* complementario; mientras que el primero es indispensable para el funcionamiento en cualquier sistema informático, el segundo no lo es, y por tanto es prescindible[71].

---

[69] STOKES, J. M: *Inside the Machine: An Illustrated Introduction to Microprocessors and Computer Architecture,* Ed. No Starch Press, 1ª edición, San Francisco, 2006, pp. 320 y ss.

[70] Una cámara digital de fotografía funciona como un periférico desde el momento que se conecta a un ordenador, pero es cierto también que la propia cámara de fotos por si sola supone un sistema informático.

[71] Hoy en día se considera esencial para el funcionamiento de un sistema informático una unidad de procesamiento (*CPU*), una memoria para ejecutar las peticiones del usuario (*RAM*) y un medio de almacenamiento de información (Disco). Además suele resultar imprescindible un medio de entrada de datos (teclado) y un medio de salida de datos (pantalla o *display*). Será *hardware* no esencial cualquier otro dispositivo físico que pueda operar en el sistema informático. Para una idea general de los distintos tipos de *hardware* DEMBOWSKI, K.: *Gran libro de Hardware: Información sobre la totalidad del hardware, de rápido acceso*. Ed. Marcombo. 2ª edición, Barcelona 2003.

Se entiende, por tanto, que el *hardware* son los componentes físicos (internos o externos) de un sistema informático, cuya unión hace operativo (junto al *software)* dicho sistema.

c.1.2. Conceptos en torno a la idea de software.

La RAE define *software* como el "conjunto de programas, instrucciones y reglas informáticas para ejecutar ciertas tareas en una computadora". Por *software* nos referimos al equipamiento lógico (en contraposición al equipamiento físico) de un sistema informático y comprende el conjunto de los componentes lógicos necesarios para hacer posible la realización de tareas específicas para las que están diseñados los elementos físicos del sistema (*hardware*)[72].

Existe multitud de *software* con diferentes finalidades. El principal *software* presente en los sistemas informáticos actuales es el que realiza las funciones de sistema operativo, y es la base sobre la que el resto de los tipos de *software* trabajan; entre muchas otras aplicaciones informáticas, podemos señalar los procesadores de textos, los videojuegos, los programas de diseño gráfico o incluso las aplicaciones de programación del propio *software*[73]. Debe además extenderse la idea de *software* a las aplicaciones que permiten la interacción hombre-máquina en cualquier sistema informático, es decir, el menú desde el que se gestiona un teléfono móvil, el de una videoconsola, un cajero automático, o una fotocopiadora electrónica suponen, con mayor o menor complejidad técnica, un *software* para su utilización.

c.1.3. Conceptos en torno a la idea de sistema informático y redes informáticas.

Es común cuando nos movemos en este campo hablar indistintamente de sistemas de información o de sistemas informáticos. Aunque el concepto de

[72] STOKES, J. M: *Inside*… ob. cit. pp. 360 y ss.

[73] Generalmente podemos diferenciar *software* de sistema (aquel mínimo necesario para hacer funcionar el *hardware*, como es el sistema operativo, los controladores de los dispositivos, etc.), *software* de aplicación (una vez el sistema está en funcionamiento aquel, que aumenta las posibilidades del mismo: procesadores de texto, editores de imagen o de video, videojuegos, etc.), y *software* de programación (destinado a crear nuevo *software*). Para un tratamiento detallado se recomienda la lectura de SOMMERVILLE, I.: *Ingeniería del software*, Ed. Pearson Educación, 7ª edición, Madrid, 2005 y PRESSMAN, R. S.: *Ingeniería del Software, un enfoque práctico*, Ed. Mc Graw Hill, 7ª edición, Madrid, 2010.

"sistemas de información" no tiene que referirse exclusivamente a los sistemas informáticos[74], debemos partir de la base de que, en lo que a nuestro estudio se refiere, cuando aludíamos al concepto de sistemas de información nos vamos a referir exclusivamente al campo de la informática, puesto que no aportaría nada a la regulación la inclusión en la definición de los aspectos humanos de la toma de decisiones de los sistemas de información[75]. Así, usaremos ambos conceptos indistintamente.

Sentada esta premisa, una primera aproximación de "sistema de información" es la realizada en el *Federal Standard 1037C*[76] conforme a la cual se considera como sistema de información informático cualquier "sistema o subsistema de telecomunicaciones o computacional interconectados y que se utilicen para obtener, almacenar, manipular, administrar, mover, controlar, desplegar, intercambiar, transmitir o recibir voz y/o datos, incluyéndose en el mismo tanto los programas (*software* y *firmware*) como el equipo (*hardware*)". De esta primera definición podremos extraer en lo sucesivo que los ordenamientos jurídicos, al menos en los instrumentos relativos al Derecho penal que vamos a analizar, recogen, aunque no literalmente, los requisitos fundamentales que debe tener un sistema de información: esto es, la interconexión de uno o varios equipos, sus elementos tanto físicos como lógicos (el equipo en sí, y los programas que lo hacen manejable para los usuarios), y

[74] LAPIEDRA ALCAMÍ, R.: "Diferencia entre Sistema Informático y Sistema de Información" en *Cámara de Comercio de Valencia-Artículos Empresariales*, nº 3-1454-10-2002, 2002, (sin numerar) "un sistema de información es algo más que un sistema computerizado *(informático)*. El sistema de información es indisociable del sistema organización-entorno, y en el proceso de adopción de decisiones no se puede pretender que toda la información necesaria sea predeterminada, formalizada e informatizada".

[75] Los delitos que tratamos en esta investigación tienen por objeto el ataque a sistemas informáticos que podrían formar parte de un sistema de información, aunque no sería necesario. Como hemos puntualizado, el sistema de información está compuesto por una parte informatizada (el sistema informático) y una parte humana. Por tanto, aunque esa parte humana que utiliza el sistema informático puede ser objeto de acciones típicas, a través de los delitos de coacciones o amenazas, lo que ahora interesa en este desarrollo son aquellos delitos que afectan directamente a la parte informática.

[76] Llamado "*Telecommunications: Glossary of Telecommunication Terms"*. Es un estándar federal realizado por la "*General Services Administration"* de acuerdo con la "*Federal Property and Administrative Services Act"* de 1949. Este documento ha sido utilizado por toda la administración norteamericana a modo de glosario para establecer unidad a la hora de definir los conceptos relacionados con la materia informática y de telecomunicaciones hasta el año 2001 en el que fue sustituido por un nuevo estándar.

una serie de posibilidades que nos permiten esos equipos (modificación, envío, almacenamiento de datos, etc.). En la actualidad el *Federal Standard 1037C,* con origen en las instituciones gubernamentales americanas, ha sido sustituido por un nuevo estándar, elaborado por el *American National Standards Institute*[77]. El nuevo estándar recoge literalmente la definición de su predecesor, lo que hace pensar que esa definición se puede considerar como definitiva. Un tercer estándar, el MIL-STD-188[78] utiliza para la definición de sistemas de información en el campo militar una adaptación del concepto de los previamente referidos estándares cuyos elementos son principalmente los ya citados. Por último, la también americana CNSS[79] mantiene una definición de sistemas de información que en su redacción de 2010 se ha simplificado, pero sigue manteniéndose fiel a la definición original[80].

En Europa, a diferencia de los Estados Unidos, no ha existido una concreción terminológica basada en estándares, y no encontramos por tanto una definición satisfactoria o mínimamente común sobre lo que se debe entender por sistema de información. Una fuente aproximada es la derivada del Convenio del Consejo de Europa sobre la Ciberdelincuencia de Budapest, de 23 de junio de 2001, en el que establece como tal "todo dispositivo aislado o conjunto de dispositivos interconectados o relacionados entre sí, siempre que uno o varios de ellos permitan el tratamiento automatizado de datos en ejecución de un programa." Es la mejor aproximación a una definición común para los Estados europeos (y no europeos) que

[77] Llamado *T1.523-2001, Telecom Glossary 2000*. Sus definiciones son utilizadas como el estándar actual, si bien a diferencia de su predecesora, la *American National Standards Institute,* tiene un carácter privado sin ánimo de lucro, aunque entre sus participantes se encuentran principalmente agencias gubernamentales, así como otras organizaciones de profesionales y académicos, y como ella misma se autodefine busca el desarrollo de normas voluntarias de consenso sobre productos tanto a nivel nacional como internacional.

[78] Estándar de carácter militar desarrollado por el Departamento de Defensa de los Estados Unidos a través de la *Defense Information Systems Agency* donde se recoge que el sistema de información de defensa se trata de una herramienta de transferencia diseñada para enviar por el sistema de punto a punto, datos y voz, imágenes, video y teleconferencia entre los operadores del Departamento de Defensa.

[79] Siglas en inglés de *Comitte On National Security System*, organización intergubernamental del gobierno de Estados Unidos cuya misión es establecer los mecanismos de seguridad en los sistemas de información norteamericanos.

[80] Lo define como un conjunto definido de recursos de información separados unos de otros y organizados para la recolección, procesamiento, mantenimiento, uso, distribución, difusión y disposición de la información.

podía encontrarse hasta la fecha de aprobación de la Decisión Marco 2005/222/JAI del Consejo, de 24 de febrero de 2005 relativa a los ataques contra los sistemas de información, que en una línea similar lo define como "todo aparato o grupo de aparatos interconectados o relacionados entre sí, uno o varios de los cuales realizan, mediante un programa, el tratamiento automático de datos informáticos, así como los datos informáticos almacenados, tratados, recuperados o transmitidos por estos últimos para su funcionamiento, utilización, protección y mantenimiento".

Por tanto, podemos establecer como válidas las definiciones que los diferentes estándares americanos han dado, así como las originadas en otros ámbitos como el europeo, por cuanto entendemos que ante la falta de crítica a tales definiciones, se puede interpretar que es un término con un amplio consenso a nivel gubernamental, empresarial, etc. Cabría preguntarse en todo caso por qué la legislación española en el ámbito penal, en cambio, y aunque ya hemos señalado que su significado debe ser considerado equivalente, ha preferido utilizar la expresión sistema informático, apartándose de la línea del Convenio de 2001 y la Unión Europea

Sobre este concepto, por último, debe insistirse en la idea de que cuando hablamos de sistema de información, hoy en día, no debemos limitarlo a la idea de ordenador. Un sistema de información debe ser considerado todo conjunto *hardware-software* operativo. Así lo entiende además el legislador español en la actual regulación penal al referirse a los daños cometidos sobre sistemas informáticos, y no meramente ordenadores. La protección penal del artículo 264 CP es por tanto la misma ya nos refiramos a ordenadores, teléfonos móviles, videoconsolas o cualquier otro dispositivo *hardware-software*. Hace además una equiparación adecuada, al proteger los datos informáticos de esos sistemas, por lo que sitúa a los datos informáticos de cualquier tipo de sistema informático al que nos refiramos en un plano de igual protección[81]. De estas ideas se puede hacer una primera aproximación, que desarrollaremos más tarde, sobre la amplitud de aparatos a los que nos referimos cuando hablamos de un sistema informático.

[81] Esto parece del todo lógico vista la evolución de la informática en la actualidad. Por ejemplo, el mismo documento electrónico puede encontrarse en un ordenador, en un teléfono móvil, en un libro electrónico, etc., y por tanto su protección debe ser la misma en todos los casos.

Por otro lado, las redes informáticas[82] suponen una serie de sistemas informáticos (por tanto, no sólo ordenadores) conectados entre sí por medio de dispositivos físicos que envían y reciben información a través de cualquier medio hábil para el transporte de datos, con la finalidad de compartir recursos y ofrecer servicios[83]. Paradigma de las redes informáticas es Internet[84], una red informática de extensión global que conecta sistemas informáticos en todas las partes del mundo. En relación con Internet habitualmente se utiliza el término ciberespacio, aunque no son del todo comparables[85], ya que a partir de este segundo concepto giran otras ideas relacionadas con campos más allá de la informática y las redes como pueden ser el político, el filosófico, el comercial o el jurídico[86]. Así por ejemplo, el Convenio

[82] Del inglés *networks*, en castellano no existe un vocablo para referirse al mismo significado. De hecho, por sorprendente que parezca tampoco en la definición que la RAE realiza de la palabra red se encuentra una acepción referida a las redes informáticas. El funcionamiento básico de una red informática basada en línea de teléfono se puede ver en VILLÉN SOTOMAYOR, M.: "La red y su evolución y utilización para actividades ilícitas" en VELASCO NÚÑEZ, E. (dir.): *Delitos contra y a través de las nuevas tecnologías. ¿Cómo reducir su impunidad?*, Ed. Consejo General del Poder Judicial, Cuadernos de Derecho Judicial, 1ª edición, Madrid, 2006, pp. 13-37.

[83] TANENBAUM, A. S.: *Redes de computadoras*, Ed. Pearson Educación, 4ª edición, Madrid, 2003, p. 3.

[84] Ya se ha explicado su origen y evolución en esta investigación. Para un mayor conocimiento sobre su funcionamiento en la actualidad se recomienda, PIQUERES CASTELLOTE, F.: "Conocimientos básicos en Internet y utilización para actividades ilícitas" en VELASCO NÚÑEZ, E. (dir.): *Delitos contra y a través de las nuevas tecnologías. ¿Cómo reducir su impunidad?*, Ed. Consejo General del Poder Judicial, Cuadernos de Derecho Judicial, 1ª edición, Madrid, 2006, pp. 42 y ss.

[85] La palabra ciberespacio fue popularizada por William Gibson en su novela de 1984 *Neuromante* aunque su origen es incluso anterior, utilizado en un cuento corto del mismo autor titulado *Johnny Mnemonic* de 1981. Refiriéndose a Internet como el ciberespacio MUÑOZ MACHADO, S.: *La regulación…* ob. cit. p. 7 señala que "es una infraestructura universal, a través de la cual se emite y recibe voz, texto e imágenes con origen y destino en cualquier lugar del mundo. Está instalado sin tener en cuenta las fronteras de los Estados porque supera el espacio físico sobre el que están constituidos los Estados. Estamos ante un territorio abierto, el Ciberespacio es un mundo sin fronteras".

[86] Baste ahora señalar algunas reflexiones sobre el ciberespacio más allá de su componente técnico. PÉREZ LUÑO, A. E.: "Internet y Derecho" en *Informática y Derecho, Jornadas marco legal y deontológico de la Informática*, nº 19-22, 1998, p. 722, afirma que "el Ciberespacio es un microcosmos digital en el que no existen fronteras, distancias ni autoridad centralizada"; por su parte GARCÍA MEXÍA, P.: *Principios de Derecho de Internet*, Ed. Tirant lo Blanch, 2ª edición, Valencia, 2005, p. 102, reconoce que "en el seno de la red desaparece el concepto de frontera geográfica. En el mundo real la frontera geográfica continúa y continuará siendo mucho tiempo un factor esencial, ya sirva para delimitar ámbitos de poder y jurisdicción de Estados, ya de organizaciones supranacionales más o menos integradas; por último desde un punto ético-filosófico BALLESTEROS LLOMPART, J.: "Filosofía del Derecho, conciencia ecológica y universalismo ético" en *Diálogo filosófico*, nº Enero-Abril 2003, p. 30, comenta que "en relación con la búsqueda de lo nuevo, el sentido de la filosofía del

internacional más importante en materia de protección penal de los sistemas informáticos incluye en su título la palabra "ciberdelincuencia" y no delincuencia informática o delincuencia de sistemas informáticos, aunque si bien es cierto, suelen utilizarse con significados análogos[87].

c.2. *Hackers, crackers* y otros sujetos asociados a la informática.

Una de las cuestiones más controvertidas, y que trataremos en esta investigación desde diferentes puntos de vista, es el papel que desempeñan en la actual sociedad informatizada determinados sujetos con avanzados conocimientos técnicos sobre la materia. La RAE no contiene una palabra para sujetos con altos conocimientos en seguridad informática, redes y computadoras, por lo que en castellano se suele utilizar la palabra en inglés *hacker;* en todo caso es común asociar la palabra *hacker* a la de pirata informático (acepción de pirata que tampoco recoge el diccionario de la RAE). Pero no se debe confundir, pues no todo *hacker* es un pirata informático, aunque sí se puede decir que el pirata informático comparte en alguna medida conocimientos *hackers* para realizar sus actividades ilícitas.

En general, el conocimiento general de la sociedad asocia *hacker* con acciones delictivas, aunque éstas no siempre tienen un reproche social notorio. Este es el caso de aquellos *hackers* que vulneran la seguridad de sistemas informáticos con intención de descubrir fallos en los sistemas de seguridad sin intención de beneficiarse de dichos fallos o, por otro lado, aquellos *hackers* que dirigen sus ataques contra sujetos con mala fama entre la sociedad (grandes empresas, partidos

---

Derecho debería consistir en descubrir cuáles son las nuevas víctimas que aparecen en relación con los nuevos cambios experimentados con la aparición de las nuevas tecnologías, sin olvidarse naturalmente de las víctimas de siempre". Para entender la trascendencia social, más allá de la técnica, del ciberespacio se antoja como lectura muy recomendada NORA, D.: *La Conquista Del Ciberespacio*, Ed. Andrés Bello, 1ª edición, Barcelona, 1997.

[87] Desde una primera visión aproximada la ciberdelincuencia subsume tres tipos de actividades delictivas: las primeras, relativas a formas tradicionales de delincuencia en las que aparecen ahora los sistemas informáticos o redes de comunicaciones; las segundas, relacionadas con la publicación de contenidos ilegales; y las terceras, relacionadas con los ataques a sistemas de información (artículo –sin firma- "¿Qué es la ciberdelincuencia?" en *Cuadernos de criminología: revista de criminología y ciencias forenses*, nº 9, 2010, pp. 32 y 33). Por su parte la COM(2007)267 final, de 22 de mayo de 2007, determina que por ciberdelincuencia se entienden las "actividades delictivas realizadas con ayuda de redes de comunicaciones y sistemas de información electrónicos o contra tales redes y sistemas"

políticos u otras asociaciones), cuyo activismo produce en mayor o menor medida daños económicos cuantificables. Es cierto, además, que no todas las actividades de los *hackers* son ilícitas o delictivas. Detrás de esta no tan mala fama de los *hackers* se encuentra lo que se ha venido a denominar la ética *hacker*[88], que entre otras cosas hace una clasificación de los diferentes tipos de *hackers* en función de las acciones que llevan a cabo[89]. No obstante esta clasificación puede resultar engañosa, pues tanto la moral del *hacker* como las acciones derivadas de ella, no por estar exentas de mala intención, debe entenderse que sean siempre lícitas[90].

A lo largo del estudio comprobaremos qué acciones llevadas a cabo por los denominados *hackers* pueden ser consideradas un acto delictivo y cuáles por el contrario no lo son. También descubriremos que, tal y como están regulados los delitos informáticos en la actualidad en nuestro Código penal, no siempre hace falta ser uno de estos sujetos con elevados conocimientos sobre sistemas informáticos para cometer los diferentes delitos de daños informáticos tipificados.

---

[88] GALINDO GARCÍA, A.: "Ética e Internet: una apuesta a favor de la verdad y de la solidaridad comunicativas", en *Salmanticensis, Universidad Pontificia de Salamanca*, nº. 44.2, 1997 p. 257. Véase también HIMANEN, P.: *La ética del hacker y el espíritu de la era de la información*, Ed. Destino, 1ª edición, Barcelona, 2002.

[89] Personas que se dedican por vocación a la seguridad informática entre las que se pueden encontrar los llamados *Black hats* cuya finalidad podría describirse de dudosamente ética o lícita, y conocidos generalmente como *crackers*; pero también los denominados *White hats*, que dedican sus conocimientos a depurar y arreglar errores en los sistemas; entre ambos tipos los llamados *Grey hats* cuyas intenciones se encuentran a medio camino de los anteriores. MOORE, R.: *Cybercrime: Investigating High Technology Computer Crime*, Ed. Elsevier, 2ª edición, Nueva York, 2010, pp. 265 y ss.

[90] Sin entrar ahora en un análisis profundo, la actual regulación de los delitos de descubrimiento y revelación de secretos del artículo 197.3CP (en vigor tras la entrada en vigor de la LO 5/2010 de 22 de junio), castiga "el que por cualquier medio o procedimiento y vulnerando las medidas de seguridad establecidas para impedirlo, acceda sin autorización a datos o programas informáticos contenidos en un sistema informático o en parte del mismo o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho a excluirlo, será castigado con pena de prisión de seis meses a dos años", es decir, la mera presencia de un tercero sin autorización en un sistema informático podría ser constitutiva de delito, aunque no se produzcan daños, o incluso aunque la finalidad del tercero sea advertir al propietario del fallo de seguridad en su sistema; actividad bastante frecuente de los denominados *White hats Hackers* en la que descubren fallos de seguridad de sistemas informáticos y ponen en conocimiento público que existe dicho fallo (pero no como aprovecharlo).

3. LA INFORMÁTICA COMO FUENTE DE ABUSOS

Ya hemos visto que la informática moderna, así como Internet, se desarrollan fundamentalmente en los Estados Unidos de América entre las décadas de 1940 y 1980, siendo a partir de 1970 cuando se implanta la idea de hacer llegar los ordenadores personales a los hogares de los ciudadanos y no concebir la informática únicamente como una herramienta de las administraciones o de las universidades.

Los casos de abusos sobre sistemas informáticos tienen su inicio de forma paralela también en los Estados Unidos de América y hoy en día son asociados con el muy amplio término de virus informáticos[91]. En efecto, el concepto de virus informático es quizá demasiado amplio, y engloba muchos tipos de métodos para cometer los abusos sobre los sistemas informáticos; no sólo ello, sino que además no todos los abusos sobre sistemas informáticos son consecuencia de la actuación de un virus. Resulta notorio que ninguno de los principales países europeos, ni Estados Unidos, hayan incluido en su regulación penal este concepto. En general dichas regulaciones -la española también- han preferido siempre definir los daños informáticos a partir del resultado finalmente acaecido[92]. No obstante, en una cantidad significativa de ataques informáticos el elemento lógico que produce el daño puede ser considerado un virus, por lo que cabe hacer ahora una aproximación a lo que dicho concepto significa y cual es su evolución desde su aparición por primera

[91] Cuando lo cierto es que no todos los abusos informáticos están vinculados con el uso de virus informáticos. Así, existen otras formas de realizar ilícitos en Internet sin necesidad de éstos (explotación de vulnerabilidades) o, aun utilizando *software* malicioso, que difícilmente se pueda considerar el mismo como virus informáticos (ataques de denegación de servicios o aprovechamiento de vulnerabilidades). Se puede ver una radiografía general sobre los abusos informáticos, lejos del ámbito jurídico, en WALL, D. S.: *Cybercrime*. *The transformation of crime in the information age*, Ed. Polity Press, 1ª edición, Cambridge, 2007 y YAR, M.: *Cybercrime and society*, Ed. Sage, 1ª edición, Londres, 2006.

[92] En el StGB en sus parágrafos §303a y §303b, se expresa la idea de dañar datos y obstaculizar sistemas informáticos, pero no establece en ningún momento el modo de hacerlo, ni menciona la utilización de virus informáticos o *software* malicioso para ello. En el mismo sentido el Código penal italiano en los artículos 635bis, 635ter y 635quarter y 635quinquies. En la regulación francesa, se sanciona expresamente a los que faciliten la comisión de los delitos informáticos a través de "un instrumento, un programa de ordenador o datos diseñados o adaptados" para cometerlos en su artículo 323-3-1. En la misma línea, pero también sin mencionar el concepto de virus informáticos, el ordenamiento británico utiliza la idea de "artículos" para cometer alguna de los tipos penales de la Ley de delitos informáticos (sección 6 de la *Computer misuse offences Act*).

vez en la historia de la informática hasta nuestros días. Además, también repasaremos otro tipo de ataques informáticos en los que no se produce la participación de un virus informático, pero se puede producir igualmente un resultado dañino.

A) HISTORIA DE LOS VIRUS INFORMÁTICOS

Lo adecuado sería empezar por determinar qué es un virus informático. Para ello podemos partir de la definición que realiza la RAE que, aunque no es totalmente adecuada por los motivos que expondremos a continuación, puede resultar orientativa. Así, para la RAE virus en su acepción referenciada con la informática es un "programa introducido subrepticiamente en la memoria de un ordenador que, al activarse, destruye total o parcialmente la información almacenada". En principio es correcto el determinar que un virus es un programa, o *software*, que actúa sobre el *software* del sistema informático víctima alterando su normal funcionamiento. Por tanto, podemos precisar respecto a la definición de la RAE que los virus informáticos no afectan a ordenadores exclusivamente, sino a sistemas informáticos en general[93].

Además, sobre el resultado que causan se pueden hacer algunas precisiones. Un virus, de la misma forma que cualquier otro *software*, siempre va a alterar la información contenida en la memoria de un sistema, proceso que se hace en todos los casos borrando o añadiendo nuevos datos al sistema original[94]. Por ello, definir virus a partir del resultado de dañar "total o parcialmente la información almacenada" no parecería lo más adecuado, y sí en cambio redefinirlo en un plano relativo a la afectación del normal funcionamiento del sistema informático; entre otros motivos, porque un virus informático puede no destruir información, sino simplemente provocar que determinada información quede inaccesible, por tanto la definición de la RAE excluiría de la categoría de virus informático al *software* que ejecute dicha acción, lo cual por pura lógica, no es aceptable. Además, cabe señalar, en la misma línea con las ideas anteriores, que el hecho de que la forma más común que tiene un

[93] Además de virus informáticos que afectan a ordenadores, son cada vez más frecuentes virus informáticos destinados a alterar el comportamiento de *tablets*, teléfonos móviles, videoconsolas, etc.

[94] LITTLEJOHN SHINDER, D.: *Prevención y detección de delitos informáticos*, Ed. Anaya, 1ª edición, Madrid, 2003, p. 410.

virus de conseguir introducirse en un sistema informático sea "subrepticiamente", no hace de esta una característica del mismo. Un virus informático, como *software* que provoca la alteración no deseada del funcionamiento normal de un sistema informático, no deja de ser un virus en función de la diferente forma que haya tenido de acceder al sistema informático.

Por último, se puede deducir que de la actuación de un virus, al tratarse de un *software* (recordamos, elemento lógico de un sistema informático), en principio sólo se van a ver afectados por el mismo elementos lógicos, es decir, otro *software* o información almacenada en la memoria del sistema[95]. Esto excluye, en principio, la actuación directa de los virus informáticos sobre el *hardware* (parte física). En todo caso esta afirmación debe ser matizada, pues sí es posible, de forma indirecta, que la actuación de un virus informático afecte a una parte física del equipo: esto se produciría en el caso de que un virus ejecutándose en el sistema informático infectado modificara el normal funcionamiento del sistema operativo de tal forma que provocase un uso excesivo de los recursos físicos mismos; con la consecuencia de que dicho uso excesivo deviniese en una avería física de algún componente del *hardware*[96]. En todo caso, no sería un daño directo producido por el virus, sino una consecuencia secundaria del daño sobre el *software*.

Cabe señalar, por ahora de forma general, que los daños informáticos tipificados en el artículo 264 de nuestro Código penal pueden ser producidos sin género de dudas a través de la afectación de los sistemas por medio de virus informáticos. Aunque, de forma adecuada, la regulación penal no se refiere en ningún momento a la existencia de dichos virus, y se limita a expresar que la

[95] En general un virus sólo afecta a datos informáticos, esos datos informáticos pueden ser los que hacen funcionar un *software* del sistema (por ejemplo los archivos que hacen funcionar el sistema operativo) o datos informáticos que forman parte de una serie de información (por ejemplo los datos informáticos que componen un documento de texto o un video).

[96] Es posible dañar algunas partes físicas de un sistema informático, por ejemplo el disco duro, haciendo que un virus informático lea una y otra vez el mismo sector del disco, reduciendo la vida útil del mismo, y provocando finalmente el fallo mecánico del mismo. Un ejemplo algo más burdo, pero real, sería el producido por un virus informático que ejecuta la acción de expulsar la bandeja de un lector/grabador de CD/DVD y acto seguido la vuelve introducir, y así sucesivamente de forma indefinida, de tal forma que del mero uso abusivo del mecanismo de apertura/cierre de éste, se averiase.

afectación de la información de un sistema informático de alguna de las formas previstas por el tipo[97] será punible; debemos tener presente la posibilidad de que esta afectación se haya producido por la acción de estos virus informáticos. En el análisis del tipo penal que llevaremos a cabo en el capítulo tercero, nos aproximaremos en detalle a la forma y las consecuencias de las diferentes formas de afectar la información lógica contenida en un sistema informático, y también las posibles diferentes consecuencias, ante el mismo resultado, de acciones de daños informáticos producidas por virus o bien por otros medios.

a.1. El primer virus informático y evolución de los virus.

Partiendo de las ideas que acabamos de exponer debemos considerar por tanto un virus informático al *software* que al ejecutarse en un sistema altera su funcionamiento provocando que no actúe como sería lo esperado. El primer programa que realizó este tipo de conducta fue, en 1971, el programa *Creeper*, un programa experimental que afectó a un determinado modelo de ordenadores de la época y que, si bien no producía daño entendido como pérdida de la información o de la funcionalidad de los equipos, mostraba un molesto mensaje en inglés[98].

En 1981 aparece el primer virus informático para ordenadores personales que afectaba a los sistemas Apple II[99]. El virus tuvo escasa trascendencia en sí mismo, pero abrió la puerta, sin saberlo, a una nueva generación de programadores de virus

[97] El tipo penal del artículo 264 CP, como más adelante veremos, se limita a señalar que el borrado, daño, deterioro, alteración, supresión, o inaccesibilidad de la información se haga de cualquier manera, de forma que no alude específicamente que sea a través de virus informáticos, sino cualquier medio.

[98] Creado por el investigador de BBN Technologies, Bob Thomas, el programa simplemente hacía aparecer el siguiente mensaje en la pantalla del ordenador: "*I'm the creeper, catch me if you can*!" ("soy una enredadera -*creeper* en inglés-, cógeme si puedes"), RUSSELL, D. y GANGEMI, G. T.: *Computer Security Basics*. Ed. O'Reilly, 2ª edición, Sebastopol, 2006, p. 86

[99] El virus *Elk Cloner* creado por Richard Skrenta con tan sólo 15 años se distribuía a través de las unidades de disquete. El virus, concebido a modo de broma, era inocuo, pero capaz de contar el número de veces que un ordenador había sido arrancado, de tal forma que cada vez que transcurría un ciclo de cincuenta arranques de sistema mostraba el texto de un poema, BORGHELLO, C.: *Cronología de los virus informáticos: historia del malware*, Ed. Eset, edición digital, San Diego, 2012, p. 8. Disponible en http://www.eset-la.com/pdf/prensa/informe/cronologia_virus_informaticos.pdf

informáticos y, paralelamente, al desarrollo de una industria no menos importante de seguridad informática.

Pero es en 1984 cuando, por primera vez, el profesor Frederick B. Cohen de la Universidad del Sur de California denominó explícitamente con la palabra virus a los programas que se auto replicaban y alteraban el normal funcionamiento de un sistema informático[100]. Los primeros virus informáticos con verdadera trascendencia para nuestro estudio aparecen en 1986 y 1987. Si la característica de los primeros virus mencionados era que alteraban el sistema informático, pero no provocaban un daño sobre la información del mismo, la actuación de los recién aparecidos virus *Virdem*[101], *Lehigh*[102] y *Jerusalem*[103] se caracterizaba no sólo por invadir el sistema informático, los medios extraíbles y auto replicarse, sino además por producir daños al borrar información de los ordenadores infectados.

Aunque quizá el mayor punto de inflexión fue la aparición de *Morris Worm* en 1988, el primer virus que llego a infectar, gracias a la incipiente red de Internet, el 10% de los ordenadores del mundo, incluyendo terminales de la NASA o el Departamento de Defensa de los Estados Unidos. No tanto los efectos dañinos del virus, sino la velocidad de infección aprovechando vulnerabilidades en programas que permitían acceso a la red, fue lo que provocó que por primera vez se crease una

---

[100] COHEN, F. B.: "Computer Viruses - Theory and Experiments" en *Journal Computers and Security*, Ed. Elsevier Sciencie Publishers, nº 6, 1987, pp. 22-35. El texto se puede encontrar en http://all.net/books/virus/index.html

[101] Creado por el ingeniero Ralf Burger en 1986 estaba preparado para auto reproducirse y borrar archivos del sistema huésped. Suele ser considerado el primer virus dañino de la historia. BORGHELLO, C.: *Cronología*… ob. cit. pp. 12 y 13.

[102] De origen incierto, aunque circunscrito al ámbito universitario (por lo que se cree que fue un experimento para conocer el alcance y capacidad de los virus informáticos), borraba información del sistema cada vez que se cumplía un ciclo determinado de infecciones así como alteraba los datos de un disquete que se encontrase en el ordenador, BORGHELLO, C.: *Cronología*… ob. cit. pp. 13 y MATAS GARCÍA, A. M.; MÍGUEZ PÉREZ, C.; PÉREZ AGUDÍN, J.; PICOUTO RAMOS, F. y RAMOS VARÓN, A. A.: *La biblia del Hacker. Edición 2006*, Ed. Anaya Multimedia, 1ª edición, Madrid, 2006, p. 699.

[103] Aparecido en 1987, fue el primer virus famoso mundialmente por su curioso modo de operar. Más conocido como Viernes 13, fue el primero capaz de no auto ejecutarse al infectar un sistema, sino quedarse latente hasta una fecha señalada por el programador del virus (los días de la semana viernes que coincidían con el día 13 del mes), BORGHELLO, C.: *Cronología*… ob. cit. pp. 13 y MATAS GARCÍA, A. M.; MÍGUEZ PÉREZ, C.; PÉREZ AGUDÍN, J.; PICOUTO RAMOS, F. y RAMOS VARÓN, A. A.: *La biblia*… ob. cit. pp. 699 y 700.

conciencia de la importancia de protegerse contra estas amenazas, que habían pasado de convertirse en un juego entre programadores a un problema de seguridad global[104]. La aparición de estos virus realmente dañinos provocó el nacimiento de las primeras compañías informáticas especializadas en seguridad y, ya a partir de 1988, aparecen en escena los primeros programas antivirus[105].

a.2. Los virus informáticos en la actualidad.

Hasta el establecimiento de las redes informáticas, especialmente Internet, los virus tenían una capacidad de afectación limitada. Principalmente se auto replicaban en medios extraíbles del sistema -especialmente en disquetes- para luego infectar aquellos ordenadores donde esos disquetes fuesen introducidos. Además, hasta 1986 las acciones sobre los sistemas no producían daños en forma de pérdida de información. Sin embargo, a partir de 1988, con la trascendencia adquirida por el virus *Morris Worm* y la aparición de las primeras compañías informáticas dedicadas a la protección de los sistemas informáticos de sus clientes, también comienza a desarrollarse la lucha por crear virus con diferentes características, más agresivos, menos detectables y con propósitos muy variados[106].

Así, podemos decir que hoy en día existe una clasificación relativamente estable de los tipos de virus informáticos y su modo de funcionamiento, aunque es cierto que esta clasificación depende de la evolución de los métodos de abusos que se puedan desarrollar en un futuro y, conociendo la rápida evolución de la informática,

[104] BORGHELLO, C.: *Cronología*… ob. cit. p. 14 y MATAS GARCÍA, A. M.; MÍGUEZ PÉREZ, C.; PÉREZ AGUDÍN, J.; PICOUTO RAMOS, F. y RAMOS VARÓN, A. A.: *La biblia*… ob. cit. 699 y 700.

[105] La aparición de estas compañías que se dedicaban a la lucha contra los virus informáticos provocó, a su vez, una carrera técnica con algunos programadores que centraron sus esfuerzos en crear virus más destructivos y de detección más complicada. El virus *Dark Avenger* v.1800 del año 1990 estaba programado para atacar en primer lugar los datos que hacían funcionar los programas antivirus, y una vez inutilizados afectaba al resto de información del sistema, MATAS GARCÍA, A. M.; MÍGUEZ PÉREZ, C.; PÉREZ AGUDÍN, J.; PICOUTO RAMOS, F. y RAMOS VARÓN, A. A.: *La biblia*… ob. cit. pp. 700 y 701

[106] Señala acertadamente RUILOBA CASTILLA, J. C.: "La actuación policial frente a los déficits de seguridad de Internet" en *Revista de Internet, derecho y política. Revista d'internet, dret i política*, nº 2, 2006, p. 60, que "lo preocupante es el aumento de hechos que se producen en los medios empresariales para perjudicar la actividad de una empresa, ya sea obteniendo información confidencial o causándole daños que perjudiquen su imagen o actividad."

es importante señalar la relevancia de hacer una revisión de ella cada poco tiempo. La explicación, al menos general, del método de funcionamiento de cada uno parece necesaria, pues es a partir de estas cuestiones de informática general como podremos entender de forma plena la protección penal que existe en nuestro país actualmente contra estás prácticas. Por ello, lejos de tratar de establecer un análisis técnico de cada figura, sí es necesario al menos hacer esta clasificación y exponer las características de cada tipo[107].

a.2.1. Por la forma de propagación.

Una de las características fundamentales de los virus informáticos es que se auto replican y procuran su expansión en cuantos más sistemas informáticos mejor[108]. Para conseguir esto existen diferentes métodos, que no son excluyentes, y que nos permiten hacer una clasificación en torno a esta característica. Así, por un lado, encontramos los 'virus de fichero' que se caracterizan por la forma de infectar el terminal de la víctima. Se esconden detrás de archivos del sistema que en principio desempeñan funciones necesarias para el correcto funcionamiento del equipo. La infección se produce al ejecutar dichos archivos, que aparentemente pueden ser archivos de documentos de texto, archivos comprimidos, ejecutables, etc.[109] Los 'cryptovirus', similares a los anteriores, se podrían considerar un subgrupo. Se caracterizan principalmente por la dificultad de ser rastreados, ya que el fichero donde se encuentra el virus está protegido por una clave criptográfica, de tal manera que los programas antivirus no pueden detectarlo. Cuando está preparado para infectar el sistema, autodescifran su clave, realizan la infección, y vuelven a

[107] CLOUGH, B. y MUNGO, P.: *Los piratas del chip: la mafia informática al desnudo*, Ed. Ediciones B, 1ª edición, Barcelona, 1992, pp. 127 y ss. Estos problemas de seguridad ya se conocían en nuestro país en el sector de las telecomunicaciones a finales de la década de los años ochenta como se pone de manifiesto en CAMACHO LOSA, L.: *El delito informático*, Ed. Madrid, 1ª edición, Madrid, 1987, pp. 38 y ss.

[108] LITTLEJOHN SHINDER, D.: *Prevención…* ob. cit. p. 410.

[109] GUERRERO, D.: *Fraude en la red*, Ed. Ra-Ma, 1ª edición, Madrid, 2010, p. 107 y MATAS GARCÍA, A. M.; MÍGUEZ PÉREZ, C.; PÉREZ AGUDÍN, J.; PICOUTO RAMOS, F. y RAMOS VARÓN, A. A.: *La biblia…* ob. cit. pp. 706 y 707. Es el típico virus escondido en un correo electrónico en forma de archivo adjunto, se estima que a principios de siglo XXI, el 77.5% de los fallos en los sistemas de información eran debido a ellos, MAGDALENA, N.: "El cibercrimen" en *Escritura pública*, nº 16, 2002, p. 18.

encriptarse para volverse de nuevo invisibles[110]. En los 'virus polimórficos', también similares a los virus de fichero, su forma de evadir la detección es cambiando las características del propio fichero infectado original (cambiando su nombre, su ubicación en el disco o su tamaño) cada vez que se replican, de tal manera que si bien son detectables por la mayoría de los antivirus, su erradicación completa es complicada, pues mientras el antivirus elimina una de sus copias, el virus se ha replicado con otras características en otro lugar del sistema[111].

Por otro lado, algunas aplicaciones (especialmente los paquetes de ofimática: procesadores de texto, de presentaciones, hojas de cálculo, etc.) permiten la automatización de tareas del sistema a través de la creación de una serie de instrucciones denominadas macros. Pero al igual que esas instrucciones pueden estar programadas para realizar tareas de trabajo cotidiano, también pueden contener instrucciones maliciosas, que ejecuten tareas programadas que afecten a la integridad del sistema de muy diferentes maneras[112]. Éstos se pueden denominar como 'virus macro' y, en muchos casos, ni siquiera pueden ser denominados virus, sino la utilización de las ventajas de determinado *software* para generar instrucciones maliciosas que pongan en peligro la integridad de los sistemas.

Por último, los 'gusanos' (*worms*), que pueden utilizar cualquiera de las técnicas anteriores, se caracterizan por su rápida propagación utilizando generalmente las posibilidades que ofrecen las redes informáticas, especialmente Internet[113]. Así consigue autorreplicarse en los ordenadores de las víctimas que estén de alguna manera vinculadas al ordenador infectado (por ejemplo abriendo los

---

[110] MATAS GARCÍA, A. M.; MÍGUEZ PÉREZ, C.; PÉREZ AGUDÍN, J.; PICOUTO RAMOS, F. y RAMOS VARÓN, A. A.: *La biblia…* ob. cit. p. 707.

[111] GUERRERO, D.: *Fraude…* ob. cit. p. 111 y MATAS GARCÍA, A. M.; MÍGUEZ PÉREZ, C.; PÉREZ AGUDÍN, J.; PICOUTO RAMOS, F. y RAMOS VARÓN, A. A.: *La biblia…* ob. cit. p. 708.

[112] GUERRERO, D.: *Fraude…* ob. cit. p. 108.

[113] Principalmente la libreta de direcciones de correo electrónico del sistema donde se encuentran alojados, pero también otras herramientas de las redes como *Netbios*, servidores FTP o *backdoors*. MATAS GARCÍA, A. M.; MÍGUEZ PÉREZ, C.; PÉREZ AGUDÍN, J.; PICOUTO RAMOS, F. y RAMOS VARÓN, A. A.: *La biblia…* ob. cit. pp. 713 y 714, señalan que "como ya se ha comentado, su objetivo es la propagación. Es por ello que en más de una ocasión utilizando un recurso de conexión, como es el correo, en pocos minutos miles de computadoras se han visto afectadas por la plaga del gusano". También en LITTLEJOHN SHINDER, D.: *Prevención…* ob. cit. p. 411.

correos electrónicos que le envía ese sistema infectado, o descargando archivos desde un servidor FTP de ese mismo sistema) y, una vez en el nuevo dispositivo, repetir el proceso anterior y seguir expandiéndose por nuevos sistemas. Es el método por excelencia de propagación de virus informáticos hoy en día, y puede afectar además a la capacidad de las redes, pues colapsa los servidores al estar reenviándose constantemente, y a la de los ordenadores que están constantemente ejecutando sus rutinas de autopropagación[114]. Los virus más importantes a partir del siglo XXI han tomado generalmente la forma de gusano para expandirse[115].

a.2.2. Por el efecto en el sistema.

En general todos estos virus tienen una característica en común, y es que afectan a la integridad de la información del sistema, de tal forma que según la programación que tenga el virus que esté atacando se puedan producir pérdidas de información más o menos graves: la desaparición definitiva de los datos, un borrado recuperable o simplemente la inaccesibilidad a los mismos: los 'virus de *boot*' o de sector de arranque son los virus que atacan la información (datos informáticos) del sector de arranque del sistema operativo de un sistema informático; como consecuencia de dicho ataque el sistema operativo no puede arrancar y, por lo tanto, el acceso al resto de información almacenada en el sistema queda, en principio, inaccesible. Es importante señalar que este ataque sólo altera la información relativa al arranque del sistema operativo, por lo que el resto de información del disco, aunque inaccesible, no ha desaparecido y se puede recuperar[116].

De una naturaleza similar a la anterior son los 'virus FAT', que atacan los datos del disco en los que se encuentra la información sobre el lugar que ocupan el

[114] GUERRERO, D.: *Fraude…* ob. cit. pp. 109 y 110 y MATAS GARCÍA, A. M.; MÍGUEZ PÉREZ, C.; PÉREZ AGUDÍN, J.; PICOUTO RAMOS, F. y RAMOS VARÓN, A. A.: *La biblia…* ob. cit. p. 714.

[115] Uno de los más famosos virus de la historia es el denominado ILOVEYOU aparecido en el año 2000, que además de ser un virus gusano por su forma de propagación, una vez en el sistema víctima borraba principalmente los archivos de imágenes y de sonido, lo que creó una alerta social -mundial- considerable en un mundo en el que las personas empezaban a almacenar grandes cantidades de fotografías y canciones en los ordenadores, GUERRERO, D.: *Fraude…* ob. cit. pp. 109 y 110 y MATAS GARCÍA, A. M.; MÍGUEZ PÉREZ, C.; PÉREZ AGUDÍN, J.; PICOUTO RAMOS, F. y RAMOS VARÓN, A. A.: *La biblia…* ob. cit. pp. 725 y ss. y BORGHELLO, C.: *Cronología…* ob. cit. p. 24.

[116] GUERRERO, D.: *Fraude…* ob. cit. p. 107.

resto de datos en la superficie del disco. De este modo, al igual que los anteriores, sin dañar la mayor parte de la información del disco, sí se convierte ésta en inaccesible. La recuperación de los datos que se han convertido en inaccesibles se hace más complicada que en el caso anterior, pero posible en la mayoría de las situaciones[117].

En cambio, los más comunes hoy en día son el grupo de 'virus que atacan archivos concretos'. Estos virus informáticos se caracterizan por atacar uno o varios archivos de determinado tipo. En general se pueden diferenciar dos estilos de ataque: por un lado, los que atacan archivos del sistema operativo y los programas, dejándolos inoperativos y, por otro lado, los que en lugar de agredir los archivos del sistema atacan a los archivos de contenido del usuario alojados en el sistema, principalmente archivos de imagen, de audio, de video, documentos de texto, etc.[118]. Lógicamente también existen los que atentan contra ambos tipos de archivos, o sólo unos muy concretos[119]

Junto con los anteriores, los virus de mayor difusión en la actualidad son los denominados 'troyanos'. Es uno de los tipos de virus por excelencia. Recibe el nombre de la Odisea de Homero sobre la historia del Caballo de Troya. Esto es debido a que de forma análoga al pasaje legendario, estos programas generalmente infectan el sistema atacado a través de la instalación voluntaria de algún *software* por parte del usuario al que se le ha hecho creer que conseguiría unas funcionalidades positivas por instalar dicho programa[120]. La peligrosidad de este tipo de virus informáticos se deriva de la posibilidad que confieren al atacante de acceder a nuestro sistema. Al contrario que los tipos de virus que hemos analizado

[117] GUERRERO, D.: *Fraude…* ob. cit. p. 111.

[118] MATAS GARCÍA, A. M.; MÍGUEZ PÉREZ, C.; PÉREZ AGUDÍN, J.; PICOUTO RAMOS, F. y RAMOS VARÓN, A. A.: *La biblia…* ob. cit. pp. 706 y 707.

[119] La variante más extendida del ya mencionado virus ILOVEYOU borraba exclusivamente archivos de imagen (JPG) y de audio (MP3), no provocando otros daños de especial trascendencia ya que no colapsaba notablemente la conexión a la red, ni afectaba a la integridad del sistema operativo u otros programas, ni al resto de archivos de información como documentos de texto, archivos de video, etc.

[120] KURTZ, G.; MCCLURE, S. y SCAMBRAY, J.: *Hackers 2. Secretos y soluciones para la seguridad de redes*, Ed. Mcgraw-Hill, 1ª edición, Madrid, 2001, p. 619, "es un programa que aparenta ser una útil herramienta de *software* pero, en realidad, cuando se ejecuta instala de forma solapada un *software* dañino o malvado o realiza acciones no autorizadas".

anteriormente, que provocan sus daños de forma automática al ejecutarse en el sistema víctima[121], en el caso de los troyanos el efecto que realmente tiene su instalación en el sistema (la infección), es crear un vínculo entre el ordenador del atacante y el ordenador de la víctima de tal forma que, en función de la habilidad del programador del troyano, se tenga mayor o menor acceso a los recursos y la información del sistema atacado[122]. Su propósito, por tanto, va más allá de la mera propagación y destrucción de información, y busca proveer al atacante del control absoluto del equipo donde reside[123], pudiendo éste realizar además de las acciones habituales de afectación de la información, conseguir claves de seguridad o utilizar el sistema de la víctima para atacar otros objetivos procurándose el anonimato. Desde un plano jurídico aproximado podemos afirmar que las repercusiones penales de las acciones de estos tipos de virus pueden ser muy variadas, desde delitos de daños informáticos, hasta fraudes o delitos contra la intimidad.

a.2.3. Variantes combinadas.

La realidad ante la que nos encontramos en el día a día es que pocos o casi ningún virus que pretenda afectar a los sistemas informáticos en la actualidad presentan características únicamente de uno de los tipos enumerados. Lo habitual es

[121] Momento que no siempre coincide con el de la infección. Las llamadas bombas lógicas, una vez han infectado el sistema, quedan en estado de suspensión hasta que se produce un determinado acontecimiento, siendo entonces cuando despliegan sus efectos dañinos.

[122] Existen multitud de funciones que pueden ser realizadas por un virus troyano. En general las más comunes son: realizar ataques directos contra el sistema afectando a la información del mismo, realizar ataques distribuidos o de denegación de servicios hacia otros sistemas de la red (si la red es Internet, entonces a cualquier otro sistema conectado a Internet), capturar audio y video de los sistemas afectados (captura de imágenes de las víctimas activando su *webcam* por ejemplo), conseguir contraseñas o conseguir información general de la víctima con la que traficar posteriormente, etc., MATAS GARCÍA, A. M.; MÍGUEZ PÉREZ, C.; PÉREZ AGUDÍN, J.; PICOUTO RAMOS, F. y RAMOS VARÓN, A. A.: *La biblia…* ob. cit. pp. 743 y ss.

[123] Podemos entender fácilmente de lo que estamos hablando si pensamos en los sistemas de asistencia remota a través de las redes. Es habitual que en la administración pública o en la empresa privada, para evitar costes de desplazamiento y de mano de obra, los técnicos informáticos se conecten al sistema que requiere supervisión desde un ordenador central y hagan las tareas de mantenimiento que sean necesarias remotamente, de forma que no tienen que estar físicamente en el lugar donde se encuentra el terminal. Aprovechando esta idea de asistencia remota, la forma de actuar de los troyanos es muy similar, pero su ejecución normalmente se hace oculta al usuario del sistema, que no es consciente de que está siendo monitorizado ni de que su equipo está siendo manipulado por un tercero.

que los virus informáticos realicen varios ataques al sistema al mismo tiempo, y su medio de propagación no sea uno, sino todos los posibles[124]. La capacidad de crear virus más complejos radica, finalmente, en la capacidad y los conocimientos de los programadores que los elaboran y en la forma en que éstos tengan pensado utilizar dichos virus[125].

B) OTROS ATAQUES INFORMÁTICOS

Aunque los virus informáticos son uno de los medios más comunes de violar la integridad y funcionalidad de un sistema informático, en la actualidad no son el único método para hacerlo, ya que se han desarrollado otro tipo de técnicas para poder realizar abusos en sistemas ajenos de forma independiente de los virus o en complemento de la labor de éstos. Al igual que señalamos en el apartado anterior, no se trata ahora de hacer una iniciación a la práctica *hacker*, pero una clasificación adecuada y una explicación básica de cada conducta parece útil para entender de forma completa el reproche penal que de estas acciones se hace en nuestra legislación.

b.1. Hacking web.

Uno de los más frecuentes tipos de abusos que se cometen a través de los sistemas informáticos tiene como objetivo las páginas web. Hoy en día las webs de Internet ofrecen multitud de servicios al ciudadano, a la Administración, a la empresa privada, etc. No sólo hablamos de la web como el lugar donde conseguir información sobre determinados aspectos, sino de una autentica herramienta desde la que poder realizar una cantidad de trámites casi inimaginable. Pensemos por ejemplo en páginas webs que ofrecen servicios bancarios, supermercados, trámites con la

[124] GUERRERO, D.: *Fraude*... ob. cit. p. 110, "son virus multipropósito, pues aúnan características de otros virus, de tal manera que atacan con varios procedimientos de forma aleatoria y simultánea". Se hace una clasificación esquemática y actualizada en FLORES PRADA, I.: *Criminalidad Informática. Aspectos sustantivos y procesales*, Ed. Tirant lo Blanch, 1ª edición, Valencia, 2012, pp. 184 y ss.

[125] Algunos ejemplos recientes de ataques realizados a través de virus informáticos o *software* malicioso se pueden ver en GARCÍA, M.: "La nueva cara del cibercrimen" en *Byte España*, nº 196, 2012, p. 61. También en HUGHES, L. A. y DE LONE, G. J.: "Virus, Worms, and Trojan Horses. Serious Crimes, Nuisance or both?" en *Social Science Computer Review*, vol. 25, nº 1, 2007 pp. 76 y ss.

administración, con la universidad, servicios de correo electrónico, de juego en línea o almacenamiento en la nube, etc.[126]

La característica común de todos ellos es que la interacción hombre-máquina se realiza a través de un navegador -o asimilado[127]- en el que el servicio que se nos ofrece está realmente alojado en algún servidor que puede estar a miles de kilómetros de nuestro terminal[128]. Una vez asentado este concepto, imaginemos la trascendencia global que tendría un ataque informático que tuviese por objetivo, no el sistema informático de cada usuario, sino el sistema informático que gestiona los servicios que se nos ofrecen. Un solo ataque contra esta estructura podría afectar a la prestación del servicio y a los datos de todos los usuarios que lo utilizan, provocando además la total indefensión -incluso el desconocimiento- de éstos[129].

b.1.1. Ataques de denegación de servicios o DDoS no intrusivos.

Han adquirido notable relevancia en la actualidad los ataques de denegación de servicios o DDoS gracias a la facilidad con que pueden ser llevados a cabo por los

---

[126] PRIETO CAMPOS, B. y PRIETO ESPINOSA, A.: *Conceptos de informática*, Ed. McGraw-Hill, 1ª edición, Madrid, 2005, p. 281, y MATAS GARCÍA, A. M.; MÍGUEZ PÉREZ, C.; PÉREZ AGUDÍN, J.; PICOUTO RAMOS, F. y RAMOS VARÓN, A. A.: *La biblia…* ob. cit. p. 680.

[127] Por ejemplo en los teléfonos móviles o en las videoconsolas se realiza a través de una aplicación (generalmente conocida como *app*), que hace las funciones del navegador en un ordenador.

[128] El esquema básico sería entonces doble, hombre-máquina y máquina-máquina, donde la primera máquina es nuestro sistema informático (ordenador, teléfono, videoconsola, etc.) y la segunda máquina es el servidor donde se aloja la página web y el servicio que nos ofrece y queremos utilizar. La primera y la segunda máquina utilizan Internet como medio de comunicación.

[129] Esto ya ha ocurrido y ocurre con cierta frecuencia en la actualidad. Algunos de los ataques más importantes han sido: el ataque realizado contra Yahoo! el 9 de diciembre de 1997 y que dejó sin servicio a los usuarios durante 15 minutos mostrándoles un mensaje de que el servicio estaría suspendido hasta la liberación de una persona detenida, o los ataques realizados a finales del año 2010 contra las webs de algunas compañías de servicios de pago por internet como Paypal, Mastercard, Visa y el banco suizo Postfinance. Quizá uno de los más sonados, por afectar a millones de jugadores online, fue el llevado a cabo contra el servicio de juego en línea de Sony, que se vio obligado a mantener inactivo el servicio durante más de un mes en la primavera de 2011. En España también se han producido este tipo de ataques: el 17 de enero de 2011 fue atacada y dejada sin servicio temporalmente la web del Senado en protesta por la aprobación de una modificación de la ley de propiedad intelectual para perseguir ciertas formas de piratería, así como la web de la embajada de Estados Unidos y de los partidos políticos que apoyaban la iniciativa; el 11 de junio de ese mismo año fue la página web de la Policía Nacional la que quedó fuera de servicio por un ataque informático. (http://www.anonops.net/). En los citados casos todos los servicios ofrecidos por éstas quedaron inutilizados.

autores[130]. Una de las características más importantes de estos ataques DDoS no intrusivos es que no vulneran la seguridad de los sistemas informáticos que pretenden atacar, sin embargo ello no impide que su efecto sea el de suspender, al menos temporalmente, la disponibilidad del servicio del prestador del mismo[131].

Aunque hay formas muy variadas de ejecutar un ataque DDoS, el que ha trascendido hoy en día es aquel basado en la petición masiva de información a determinado servidor web, generalmente el que aloja una página en Internet. En general las páginas web -así como cualquier otro servicio online- están preparadas para atender un máximo de peticiones por unidad de tiempo (es decir, si tienen más de un determinado número de visitas pueden colapsarse). Los ataques DDoS no intrusivos se realizan a partir de esta idea y consisten en generar peticiones de acceso a la información de la web de forma constante, de tal manera que el servidor donde se encuentra la web se vea superado por la cantidad de solicitudes y finalmente quede bloqueado dejando de estar, por tanto, la web operativa[132].

La forma rudimentaria de realizar estos ataques partía de la necesidad de conseguir un considerable número de personas que intentase entrar al mismo tiempo a la página web que se quiere atacar y una vez en la web, volver a cargarla una y otra vez (pulsando el botón de "actualizar" que tienen todos los navegadores"). Pero hoy en día los servidores donde se alojan páginas webs suelen estar preparados para estos

[130] DÍAZ SÁEZ, V.: "Ataques DDoS: el 'backstage' de gran parte del cibercrimen" en *Red seguridad: revista especializada en seguridad informática, protección de datos y comunicaciones*, nº 58, 2012, p.28, señala acertadamente que los múltiples motivos de los atacantes para realizar estas acciones, en los últimos tiempos, han dejado de tener una finalidad exclusivamente patrimonial para dar lugar a nuevos modos de ciberactivismo. Una clasificación muy general y, en todo caso, abierta, hace ZORRAQUINO RICO, A.: "Delitos informáticos" en *Cuadernos de derecho judicial*, nº 5, 2006, p. 166, entre empleados o ex empleados laborales, activismo político o ideológico y autores con finalidades de "emulación o supremacía" con lo que parece referirse a aquellos que sólo actúan con la finalidad de poder saberse autores de grandes colapsos informáticos.

[131] MATAS GARCÍA, A. M.; MÍGUEZ PÉREZ, C.; PÉREZ AGUDÍN, J.; PICOUTO RAMOS, F. y RAMOS VARÓN, A. A.: *La biblia…* ob. cit. p. 639, "la página Web [que] se viene abajo o deja de prestar sus servicios. Siendo por supuesto [una acción] infinitamente menos intrusiva […] puede dañar la imagen de la empresa frente a sus usuarios".

[132] Aun siendo no intrusivos, se denominan ataques DDdoS por consumo de ancho de banda por un lado, o de inanición de recursos por otro. Los primeros consumen la capacidad de ancho de banda del servidor, los segundos consumen los recursos del servidor, generalmente ambos se utilizan combinados, y su éxito depende la cantidad de peticiones que sean capaces de generar por unidad de tiempo, KURTZ, G., MCCLURE, S. y SCAMBRAY, J.: *Hackers 2…* ob. cit. pp. 539 y 540.

ataques, de tal forma que por muy rápido y muchas personas que estén constantemente tratando de acceder al servicio web, estas peticiones no lleguen a colapsar la capacidad del servidor de mostrar la página[133]. Por ello, se han desarrollado programas que al instalarlos en los sistemas informáticos de los atacantes canalizan todo el ancho de banda de sus conexiones para realizar peticiones constantes de acceso a la página que pretenden interrumpir; es decir, automatizan lo que debería realizar cada atacante manualmente, de forma que aumentan exponencialmente las peticiones de acceso y, ahora si, suelen conseguir finalmente bloquear el servidor donde se aloja el servicio o la página web e interrumpir su acceso.

Sobre la utilización de estos programas para realizar los ataques debemos señalar la preocupación de las autoridades por la utilización de virus distribuidos en forma de gusano por internet, que contienen un *software* de características de virus troyano. Los llamado *botnets* son programas que infectan los ordenadores atacados y se mantienen a la espera de que el atacante los active para realizar una determinada acción. Los *botnets* se utilizan para conseguir el anonimato por parte de los atacantes en sus actividades ilícitas (envío masivo de *spam* generalmente) y, en el caso que nos ocupa, para conseguir "voluntarios" para los ataques de denegación de servicio[134]. Ya hemos señalado que el éxito de un ataque DDoS no intrusivo radica en la cantidad de personas que se sumen al ataque, pues incluso utilizando programas que automatizan las peticiones a la página web atacada es necesario que muchas personas instalen estos programas y los ejecuten para que tenga éxito el ataque. Sin embargo, gracias a la existencia de estos *botnets*, cualquier ordenador infectado puede convertirse en un aliado del atacante principal sin que el usuario tenga siquiera conocimiento de ello. Consiguiendo una infección importante por medio de un gusano que contenga el

[133] Aun así no es raro ver páginas webs que quedan inaccesibles después de que, por ejemplo, un famoso con millones de seguidores en su red social haya recomendado visitar esa página. Los millones de seguidores bien-intencionados que quieren acceder a dicha web en un espacio de tiempo muy corto generalmente terminan por bloquear la página.

[134] Explicación y ejemplos del funcionamiento de estas redes *botnets* se pueden consultar en FERNÁNDEZ LÁZARO, F.: "La Brigada de Investigación Tecnológica: la investigación policial" en VELASCO NÚÑEZ, E. (dir.): *Delitos contra y a través de las nuevas tecnologías. ¿Cómo reducir su impunidad?*, Ed. Consejo General del Poder Judicial, Cuadernos de Derecho Judicial, 1ª edición, Madrid, 2006, pp. 143 y ss. También en DÍAZ SÁEZ, V.: "Ataques DDoS…" ob. cit. pp. 28 y 29.

programa para realizar peticiones masivas a una web, se puede conseguir un ejército de atacantes sin que éstos sean conscientes de su apoyo a los ataques de denegación de servicios[135]. Más importante que los casos de ciberactivismo resulta, en todo caso, el mercado negro que se origina en torno a las redes de sistemas informáticos infectados[136], cuyo control puede ser objeto de transacciones en el mercado negro, de tal forma que aquellos que objetivamente han realizado la infección de determinado número de máquinas vendan su control a terceros, siendo éstos los que realicen a su vez las acciones que deseen a través de dichos sistemas (fraudes, daños, ciberterrorismo, etc.)[137].

b.1.2. Ataques para acceder a los servicios e información de otros sistemas.

Pueden también llevarse acabo ataques DDoS intrusivos cuya finalidad es la misma que la anterior, pero su complejidad es mayor pues requiere de conocimientos avanzados de informática, redes, programación y bases de datos. La similitud con los anteriores es que el servicio online de la víctima (generalmente su página web) deja de estar accesible al público porque se ha colapsado; y la diferencia básica es que si bien necesitan de menos "colaboración" para ser llevados a cabo, precisan de un conocimiento mayor por parte de los atacantes por conseguir su objetivo.

Pero los ataques intrusivos de los prestadores de servicios en Internet pueden tener finalidades más complejas que el mero hecho de suspender temporalmente el servicio de determinada web. Quizá el mayor peligro al que se enfrentan usuarios, instituciones y compañías es la vulnerabilidad de sus datos ante ataques contra los

---

[135] Los sistemas informáticos infectados se denominan entonces *zombies* y sirven al propósito general del atacante a través de un ataque distribuido de denegación de servicio. Los ataques a través de usuarios *zombies* son los más frecuentes ya que permiten mantener con relativa facilidad el anonimato del atacante real, KURTZ, G.; MCCLURE, S. y SCAMBRAY, J.: *Hackers 2…* ob. cit. pp. 554 y 555, y Redes Zombie en http://cert.inteco.es/Formacion/Amenazas/botnets/.

[136] Este hecho es conocido desde hace casi una década en el ámbito empresarial, BARROSO, D.: "La radiografía del cibercrimen 2008" en *Seguritecnia: Revista decana independiente de seguridad*, nº 350, 2009, p. 30.

[137] SÁNCHEZ SISCART, J. M.: "Cibercrimen y cooperación judicial. Especial referencia a los ISP alojados en EE.UU" en *Revista del poder judicial*, nº 91, 2011, p. 31 y BARROSO, D.: "La radiografía…" ob. cit. p. 30. También en la Propuesta de Directiva relativa a ataques contra los sistemas de información de la Unión Europea, tanto en su exposición de motivos como en su articulado, se deja constancia de la preocupación de las instituciones europeas por estas redes *zombies*.

servidores donde se encuentra información sensible. Acceder a un servidor web puede permitir al atacante -además de dejar la web sin servicio- modificar la información que en ella se muestra, o conseguir datos personales de los usuarios de ese servicio (contraseñas, datos bancarios, etc.)[138].

La gran diferencia con los anteriores es que, mientras a través de los ataques de denegación de servicio no intrusivos no se accede realmente a la información del prestador de servicios en la web, sino que simplemente se bloquea su capacidad de ofrecer el servicio a los usuarios, en este tipo de prácticas intrusivas el atacante sí llega a tener acceso a los servidores y la información que estos tienen almacenada, quedando por tanto expuestos los datos de los usuarios del servicio y, en general, el funcionamiento del sitio web en cuestión. Estos ataques, aunque se pueden complementar con la ayuda de virus informáticos como los que expusimos anteriormente, generalmente se basan en la explotación de vulnerabilidades originarias de los programas que gestionan los servidores centrales donde se encuentran instalados los servicios webs de las páginas atacadas; y en conocimientos avanzados de programación y bases de datos de los atacantes, que estudian concienzudamente la arquitectura de los servidores que se disponen a atacar[139] para encontrar esas vulnerabilidades preexistentes que les permitan el acceso y su posterior explotación.

[138] En este caso puede variar mucho la relevancia social o económica del ataque. Por un lado ataques con poca trascendencia económica como pudieron ser el perpetrado contra la web oficial de las Spice Girls entre el 14 y el 16 de junio de 1997 en el que la imagen principal en la web había sido modificada para mostrar a las integrantes del grupo sin pelo o el ataque contra la web española de los premios Goya de la Academia del Cine en la noche del 19 al 20 de febrero de 2012, en el que se insertó un enlace a un video de Youtube por parte de los atacantes. Por otro, caben también ataques que pueden tener consecuencias económicas graves para los proveedores de servicios como el robo de datos bancarios que se produjo el 14 de marzo de los servidores de Bank of America o los ataques de 23 y 24 de mayo ese mismo año contra Sony, en el que se eliminaron los datos de más de 2.000 usuarios registrados en su web (http://www.anonops.net/).

[139] Es una máxima común en todo *hacker* la necesidad de un estudio concienzudo de la web que se pretende atacar antes de pasar a la acción, véase MATAS GARCÍA, A. M.; MÍGUEZ PÉREZ, C.; PÉREZ AGUDÍN, J.; PICOUTO RAMOS, F. y RAMOS VARÓN, A. A.: *La biblia…* ob. cit. pp. 109 y ss. y KURTZ, G.; MCCLURE, S. y SCAMBRAY, J.: *Hackers 2…* ob. cit. pp. 5 y ss.

b.2. Hacking *wireless*.

La tecnología inalámbrica (*wireless)* permite la creación de redes de sistemas informáticos sin que se encuentren vinculados físicamente unos con otros. Esta tecnología ha tenido un desarrollo y una implantación abrumadora desde el comienzo del siglo XXI[140]. Ahora bien, como parece una constante en informática, la masificación de una tecnología que ha permitido un desarrollo importante en la sociedad lleva aparejado el aumento de la capacidad de ciertos sujetos para utilizar, con propósitos no tan socialmente adecuados, esa misma tecnología.

Sin entrar ahora en explicaciones técnicas sobre una red inalámbrica, sí debemos señalar una serie de amenazas de seguridad que pueden aparecer en torno a la misma. El principal problema surge por la intangibilidad del medio de transmisión de los datos entre sistemas informáticos, de tal manera que cualquiera que se encuentre en el rango de emisión de la señal puede, en principio, a través de un *software* especializado[141] captar esa información que viaja por el aire, descargar una copia de la misma en su sistema (que no era, en principio, el destinado a recibirla) y conocer su contenido. Método que sería igualmente posible en una red física, pero que por la propia dificultad de acceder a los cables por los que circula la información se hace en la práctica una actividad menos común y mucho más complicada. Para evitar estas violaciones de la intimidad las redes inalámbricas suelen emitir su información cifrada, de tal forma que para conseguir acceder a esa información que viaja por las ondas sea necesario tener, al menos, unos conocimientos medios de informática, o bien, que el administrador o propietario de esa red, actúe con total negligencia dejando el acceso abierto, o con un sistema de cifrado fácilmente quebrantable.

[140] La redes tipo 802.11 son las de uso frecuente en la sociedad de la información. 802.11 es un estándar de la IEEE siglas de *Institute of Electrical and Electronics Engineers*, una asociación técnico-profesional mundial dedicada a la estandarización, MATAS GARCÍA, A. M.; MÍGUEZ PÉREZ, C.; PÉREZ AGUDÍN, J.; PICOUTO RAMOS, F. y RAMOS VARÓN, A. A.: *La biblia…* ob. cit. pp. 620 y 621.

[141] Llamados *sniffers* (no tiene una traducción exacta en castellano, aunque podría entenderse como rastreador). Estos programas, que no pueden ser considerados virus informáticos pues no cumplen un propósito de autopropagación y causación de daño sobre los sistemas infectados, son capaces de rastrear los paquetes de información que circulan por una red e interceptarlos.

Por su escasa transcendencia para nuestro estudio jurídico no cabe profundizar más en este tipo de abusos de los sistemas informáticos, aunque es importante conocer su existencia, pues en todo caso la utilización de estas técnicas podría llegar a constituir un medio para cometer otra serie de delitos, entre los que. ahora sí, se pueden encontrar los daños informáticos. Sobre este determinado aspecto sí nos detendremos al analizar los medios comisivos y los tipos de daños informáticos en sus relaciones concursales con otros tipos penales; así como en nuestra propuesta final en el último capítulo de esta investigación.

CAPÍTULO SEGUNDO: REGULACIÓN EN EL ÁMBITO INTERNACIONAL DE LA DELINCUENCIA INFORMÁTICA Y TRASCENDENCIA EN NUESTRO ESTUDIO

1. INTRODUCCIÓN

Tras la introducción al objeto de estudio realizada en el capítulo anterior, vamos ahora a iniciar un recorrido desde lo general a lo particular: desde la situación de los delitos informáticos en el plano internacional hasta el análisis jurídico-penal concreto de los delitos de daños informáticos. Si en las páginas anteriores sólo hicimos algunas menciones puntuales a la temática jurídica concreta de esta investigación, a partir de ahora el ámbito del Derecho irá copando con mayor intensidad cada uno de los extremos en los cuales nos vamos a detener.

El objetivo de este capítulo es acercar al lector a la realidad eminentemente internacional de los delitos informáticos. En primer lugar abordaremos el nacimiento del Derecho penal informático desde una perspectiva internacional. Por un lado veremos el lugar que ha ocupado en los organismos internacionales más señalados (si bien los cuales no han realizado normas de carácter imperativo sino recomendaciones e informes al respecto) y también revisaremos la implantación en los países de nuestro entorno de las primeras regulaciones en materia penal respecto de esta nueva forma de criminalidad, comenzando en los Estados Unidos de América en la mitad de la década de 1980 y continuando con la aparición de las primeras regulaciones sobre la materia en Europa a partir de ese momento[142]. En este recorrido analizaremos brevemente la situación que ha existido en nuestro país respecto de estos delitos en un primer momento, de forma que se sienten las bases para entender las novedades legislativas operadas en función de la aplicación del Derecho internacional en la materia, que han tenido lugar a partir de la aprobación del Código penal de 1995.

[142] REYNA ALFARO, L. M.: "La criminalidad…" ob. cit. p. 536.

El análisis de la regulación con carácter imperativo de los delitos informáticos en el ámbito internacional ocupará la parte central de este capítulo. La regulación penal que en la actualidad existe en España a este respecto deriva por una parte, del Convenio sobre la Ciberdelincuencia de Budapest de 23 de noviembre de 2001, en el cual, por primera vez, se sientan las bases para una regulación penal, en la medida de lo posible, común a todos los Estados firmantes más allá de las meras recomendaciones y, por otro lado, de la posterior incorporación a nuestro ordenamiento de la Decisión Marco 2005/222/JAI del Consejo de la Unión Europea de 24 de febrero. A este respecto es preceptivo también analizar la propuesta de Directiva que se encuentra en tramitación en el momento actual, cuyo objetivo es ampliar y concretar el marco penal existente, y que deberán integrar los Estados miembros, una vez más, en sus ordenamientos jurídicos.

2. ANTES DEL CONVENIO Y DE LA DECISIÓN MARCO: EL NACIMIENTO DEL DERECHO PENAL INFORMÁTICO

Tal como se anunció, comenzaremos el análisis de la regulación penal de los daños informáticos en España alejándonos en el tiempo y en el espacio del momento y lugar actual para conocer, someramente, ciertos aspectos relativos a la historia de la regulación de delitos informáticos en general en los últimos treinta años. A nivel nacional, como se podía prever, el origen lo encontramos en los Estados Unidos de América, expandiéndose luego por el resto de países de nuestro entorno. Recordamos que los primeros abusos sobre sistemas informáticos datan de mediados de la década de 1980; y antes del final de esa década la mayoría de los países de nuestro entorno ya habían formulado sus primeras regulaciones a este respecto. Sin embargo, por ser la primera institución internacional en referirse a la delincuencia informática, debemos comenzar por el papel que ha realizado la Organización de Cooperación y Desarrollo Económico (OCDE[143]) en este ámbito.

[143] La Organización para la Cooperación y el Desarrollo Económicos (OCDE) es una organización de cooperación internacional, fundada en 1960 por 18 Estados Europeos, Estados Unidos y Canadá cuyo objetivo es coordinar sus políticas económicas y sociales. Tiene sede central en París (Francia) y en la actualidad está formada por 34 Estados (http://http://www.oecd.org/about/).

A) EN EL ÁMBITO INTERNACIONAL

En el ámbito internacional es importante mencionar los informes de la OCDE y el papel de la Organización de Naciones Unidas (ONU[144]) como promotores de una cierta unificación de criterios a la hora de definir y clasificar los delitos informáticos. Las conclusiones y recomendaciones de sus diferentes informes carecen, en general, de poder impositivo sobre los ordenamientos de los Estados, pero es igualmente cierto que son las primeras herramientas con vocación de unificar un problema cuya dimensión internacional comenzaba a vislumbrarse a partir de la década de 1980.

a.1. El papel de la Organización de Cooperación y Desarrollo Económico.

En 1983 la OCDE inició un estudio centrado en la posibilidad de aplicar y armonizar, en el plano internacional, las leyes penales, a fin de luchar contra el problema del uso indebido de los programas de computación[145]. En estos primeros trabajos queda claro que las posibles implicaciones económicas de la delincuencia informática tienen carácter transnacional, cuyo principal problema es la falta de una legislación unificada que facilita la comisión de los delitos.

En 1986 la OCDE publicó el informe titulado "Delitos de informática: análisis de la normativa jurídica"[146], en el cual se hacía una lista de conductas que debían ser merecedoras de reproche penal en las legislaciones de los Estados y se reseñaban además las normas legislativas vigentes y las propuestas de reforma en diversos Estados miembros. El informe concluía, en la línea de los estudios de 1983,

[144] La Organización de las Naciones Unidas (ONU) es la mayor organización internacional en la actualidad. Se autodefine como una asociación de gobierno global que facilita la cooperación en Derecho internacional, la paz y seguridad internacional, el desarrollo económico y social, los asuntos humanitarios y los derechos humanos. La ONU fue fundada el 24 de octubre de 1945 al finalizar la Segunda Guerra Mundial en San Francisco (Estados Unidos), por 51 países. En la actualidad la ONU tiene 193 Estados miembros y su sede está en Nueva York. Además existe una segunda sede en Ginebra (Suiza) (http://www.un.org/es/aboutun/).

[145] SIEBER, U.: *The International Handbook on Computer Crime Computer-related Economic Crime and the Infringements of Privacy*, Ed. John Wiley & Sons, 1ª edición, Nueva Jersey, 1987, p. 66.

[146] OCDE: "Computer-related crime: analysis of legal policy" en ICCP - *Information, computer and communications policy,* Ed. OECD Publications and Information Centre, nº 10, Washington, 31 de agosto de 1986.

con la idea de la transnacionalidad de este tipo de delincuencia y la necesidad de caminar en la línea de una protección penal común en todos los Estados[147].

En 1992 se elaboró un conjunto de normas para la seguridad de los sistemas de información con intención de ofrecer las bases para que los Estados y el sector privado pudieran erigir un marco de seguridad para los sistemas informáticos[148]. Las directrices reconocían el uso cada vez mayor y el valor de los equipos, instalaciones, redes informáticas y de comunicación; de la información y los datos que pueden ser almacenados, tratados, recuperados o transmitidos por las mismas; el carácter internacional de los sistemas de información y su proliferación en todo el mundo, su papel cada vez más importante y la creciente dependencia de ellos a nivel nacional y de la economía internacional y el comercio; así como en la vida social, cultural y política. En ausencia de las garantías adecuadas, los datos y la información en los sistemas de información estaban expuestos con relativa sencillez a ser vulnerados en comparación con los documentos en papel. Además, existían nuevos riesgos derivados de accesos no autorizados (presenciales o remotos), apropiación indebida, alteración o destrucción, etc.

Se hacía necesario aumentar la conciencia de los riesgos recaídos sobre los sistemas de información y de las posibilidades para cubrir estos riesgos; y reconocer que las medidas y procedimientos, así como las instituciones de seguridad y protección en ese momento, no podían satisfacer adecuadamente los problemas planteados. Era necesaria, por tanto, una mayor coordinación y cooperación internacional para enfrentar los desafíos a los que la novedosa situación conducía[149].

A partir del reconocimiento de esta poco deseable situación, el informe realizaba definiciones unificadas de algunos conceptos informáticos, tales como datos informáticos, sistemas de información, disponibilidad, integridad o confidencialidad de los datos informáticos; y consagraba nueve principios necesarios

[147] OCDE: "Computer-related…" ob. cit. capítulo II.

[148] OCDE: "Guidelines for the Security of Information Systems", 1992: www.oecd.org/internet/interneteconomy/oecdguidelinesforthesecurityofinformationsystems1992.htm

[149] En OCDE: "Guidelines…" ob. cit. se evalúan estos y otros problemas de la normativa en aquel momento.

para la lucha contra la delincuencia informática en el mundo: principio de responsabilidad, principio de concienciación, principio ético, principio multidisciplinario, principio de proporcionalidad, principio de integración, principio de velocidad, principio de revaluación y principio democrático[150].

Finalmente, en el año 2002, se actualizaron las directrices elaboradas en 1992[151] para dar acomodo a los nuevos problemas planteados en esa década, especialmente los derivados de la implantación a nivel mundial de Internet y lo que esto supone para la perpetración de abusos informáticos, manteniendo la estructura originaria con nueve principios. Se realizan algunas adaptaciones de los principios originales, la integración de varios de ellos y la aparición de tres nuevos: el principio de evaluación del riesgo, el principio de diseño y realización de la seguridad y el principio de gestión de la seguridad[152].

a.2. El trabajo de la Organización de Naciones Unidas en la lucha contra la delincuencia informática.

En 1990, la ONU, en el Octavo Congreso sobre Prevención del Delito y Justicia Penal, celebrado en La Habana, destaca por primera vez la necesidad de desarrollar medios de cooperación internacional en asuntos penales relacionados con la informática que complementen los ya iniciados en otras materias. En la línea con los trabajos de la OCDE -que precisamente son citados como ejemplos de buena *praxis*- reconoce que, en la medida en que los sistemas informáticos se han

[150] En OCDE: "Guidelines…" ob. cit. se enumera el contenido de cada principio.

[151] OCDE: "Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security", 2002 (http://www.oecd.org/internet/interneteconomy/34912912.pdf), p. 12. Las directrices de 1992 fueron actualizadas, sin cambios sustanciales en el año 1997. Las nuevas directrices de 2002 en cambio sí suponían una revisión completa de las anteriores, con una nueva estructura y nuevos principios de actuación: "la presente revisión se acometió en el año 2001 por el Grupo de expertos de Seguridad de la Información y Protección de la Privacidad (WPISP), de conformidad con el mandato del Comité de Política de la información, Informática y Comunicaciones (ICCP), y acelerada tras la tragedia del 11 de septiembre. El Proyecto lo emprendió el Grupo de expertos del WPISP, que se reunió en Washington DC, el 10 y 11 de diciembre de 2001, Sydney el 12 y 13 de febrero de 2002 y París del 4 al 6 de marzo de 2002. El WPISP se reunió en París el 5 y 6 de marzo de 2002, el 22 y 23 de abril de 2002, y el 25 y 26 de junio de 2002".

[152] ALAMILLO DOMINGO, I.: "Las políticas públicas en materia de seguridad en la sociedad de la información" en *Revista de Internet, derecho y política. Revista d'internet, dret i política*, nº 9, 2009, pp. 14 y ss.

convertido en una herramienta para almacenar datos de carácter político, económico, médico, sociales y personales de naturaleza reservada, pueden resultar favorecedores de nuevos métodos de delincuencia, motivo por el cual se realiza un llamamiento a los Estados miembros, por primera vez en esta materia, con el fin de que intensifiquen sus esfuerzos para combatir eficazmente este nuevo tipo de delincuencia basada en sistemas informáticos. Establece como pasos a seguir la modernización de las leyes y procedimientos penales nacionales, la mejora de las medidas de seguridad de los sistemas informáticos y la adopción de medidas para la sensibilización de la opinión pública, así como de la formación para jueces y otros funcionarios encargados de la prevención e investigación de estos delitos (refiriéndose fundamentalmente a los Cuerpos y Fuerzas de Seguridad de cada Estado) y, por último, el fomento de los esfuerzos para la elaboración de directrices generales con vocación internacional en orden a que todos los Estados integren en sus regulaciones penales los mismos delitos con consecuencias jurídicas similares. Por último, se pide al Secretario General de la ONU que contemple la idea de elaborar y publicar para el curso 1992-1993 un documento técnico sobre la prevención y el enjuiciamiento de delitos informáticos[153].

La ONU, siguiendo una línea de trabajo similar a la de la OCDE elaboró en 1994 el "Manual de las Naciones Unidas sobre Prevención y Control de Delitos Informáticos" con intención de ofrecer las bases para que los Estados y el sector privado pudieran erigir un marco de seguridad que proteja los sistemas informáticos. Esta es una de las herramientas más importantes a nivel internacional en la lucha contra los delitos informáticos, tanto por su nivel de concreción como por realizarse en el seno de la mayor organización internacional que existe[154].

Sin embargo, en el 9º Congreso sobre Prevención del Delito y Justicia Penal, celebrado en El Cairo en 1995, no existe una especial referencia a los delitos informáticos y, aunque en numerosas partes del informe final sí se señala la importancia de la lucha internacional contra estos delitos, no se específica en el caso

[153] Informe general del 8º Congreso de las Naciones Unidas sobre Prevención del Delito y Justicia Penal, La Habana, Cuba, 27 de agosto a 7 de septiembre de 1990, pp. 149 y ss.

[154] ONU: "Manual de las Naciones Unidas sobre prevención y control de delitos informáticos" en *Revista Internacional de Política Criminal*, Ed. Naciones Unidas, nº 43 y 44, 1994.

concreto de los delitos informáticos ninguna recomendación al respecto[155]. Este hecho no deja de sorprender, pues estamos ante un momento clave tanto en el desarrollo de los sistemas informáticos en general -con una implantación masificada- y de Internet en concreto, y tan solo un año antes había sido publicado el Manual ya mencionado, lo que parece que merecería al menos un comentario durante el Congreso.

La delincuencia informática sí vuelve a ser un tema central en el 10º Congreso sobre Prevención del Delito y Justicia Penal, celebrado en Viena en el año 2000, si bien cambia la rúbrica pasando a referirse a delitos relacionados con las redes informáticas[156], lo que ya da muestra de la necesidad de realizar nuevas apreciaciones a las efectuadas en el 8º Congreso y en los trabajos de 1992 y el Manual de 1994. El informe elabora un documento anexo con el recorrido histórico que sobre la materia se ha producido en el orden internacional[157]. Una vez planteada la novedad que ha supuesto la masificación del uso de Internet, el informe general enfoca su contenido hacia la necesidad de armonizar los distintos ordenamientos nacionales no sólo en materia penal, sino también en materia procesal penal y jurisdiccional en general. La comisión de delitos a través de Internet supone que el autor del mismo se encuentre en lugares remotos, lo que dificulta no sólo la localización sino, una vez localizado, la puesta a disposición de los tribunales donde los efectos de sus acciones han tenido lugar. Concluye señalando que a los esfuerzos que se han venido haciendo en la última década deben añadirse nuevos impulsos por conseguir que Internet sea un lugar de intercambio social, económico y cultural

[155] En el Informe general del 9º Congreso de las Naciones Unidas sobre Prevención del Delito y Justicia Penal, El Cairo, Egipto, 29 de abril a 8 de mayo de 1995, p. 5, se reconoce estar "alarmado por las amenazas que plantean la delincuencia transnacional organizada, los delitos terroristas y sus vínculos, los actos de violencia en zonas urbanas, el tráfico ilícito de drogas, el tráfico ilícito de armas, el tráfico internacional de menores, el tráfico ilícito de extranjeros, los delitos económicos, la falsificación de moneda, los delitos ecológicos, la corrupción, los delitos contra el patrimonio cultural, el robo de vehículos de motor, los delitos relacionados con la informática y las telecomunicaciones, el blanqueo de dinero, la infiltración por grupos de delincuentes organizados de las economías legítimas, y por los efectos de esas actividades en la sociedad", pero no se proponen medidas concretas en este ámbito.

[156] Informe general del 10º Congreso de las Naciones Unidas sobre Prevención del Delito y Justicia Penal, Viena, Austria, 10 a 17 de abril de 2000, pp. 29 y ss.

[157] Informe A/CONF.187/10 del 10º Congreso de las Naciones Unidas sobre Prevención del Delito y Justicia Penal, Viena, Austria, 10 a 17 de abril de 2000, pp. 5 y ss.

seguro, y que en este ámbito será en el que los Estados deban aumentar sus esfuerzos y colaboración en el futuro próximo.

Si los Congresos 8º y 10º suponen los hitos más relevantes en el tratamiento e importancia que la ONU ha dedicado a la delincuencia informática, de los informes de los congresos 11º y 12º podemos señalar que la misma parece consagrarse como uno de los temas fijos en estos eventos quinquenales de las Naciones Unidas. Bajo diferentes nomenclaturas[158] la aparición de nuevos trabajos en esta materia ha acaecido de forma consecutiva en las tres ultimas ediciones, y en cuatro de los últimos cinco congresos. En cuanto al contenido de la edición de 2005[159] podemos señalar que se realiza una visión panorámica de algunas nuevas formas de delincuencia informática junto con el crecimiento de Internet: se mencionan las prácticas de utilización de identidades falsas para obtener datos íntimos como contraseñas y cuentas bancarias de las víctimas (*phishing*) sin necesidad de utilizar virus u otros programas informáticos más complejos sino el mero engaño (en ocasiones burdo) a través de la solicitud por correo electrónico u otros medios de contacto electrónico de estos datos sensibles, o la aparición de webs fraudulentas con este fin[160]. También, se hace referencia a la implantación de redes inalámbricas locales, así como la importancia de verificar el impacto de las mismas en la delincuencia informática en los próximos años. Al igual que en las ediciones anteriores, se insiste en la necesidad de colaboración entre Estados, pero también entre empresas privadas y, por primera vez, se celebra la aprobación del Convenio sobre la Ciberdelincuencia de Budapest de 23 de noviembre de 2001, aunque se muestra clara cautela sobre su eficacia a medio y largo plazo, pues todavía no ha entrado en vigor en la mayoría de países que lo han suscrito. En cuanto a la edición de 2010[161] existen pocas novedades. Una vez más se hace alusión a las

[158] Bajo la rúbrica "Seminario sobre medidas para combatir los delitos informáticos" en la 11ª edición y "Novedades recientes en el uso de la ciencia y la tecnología por los delincuentes y por las autoridades competentes en la lucha contra la delincuencia, incluido el delito cibernético" en la 12ª.

[159] Informe general del 11º Congreso de las Naciones Unidas sobre Prevención del Delito y Justicia Penal, Bangkok, Tailandia, 18 a 25 de abril de 2005, pp. 94 y ss.

[160] A este respecto, FAITH CRANOR, L.: "Delincuencia informática" en *Investigación y ciencia*, nº 402, 2010, pp. 70 y ss.

[161] Informe general del 12º Congreso de las Naciones Unidas sobre Prevención del Delito y Justicia Penal, Salvador, Brasil, 12 a 19 de abril de 2010, pp. 59 y ss.

complicaciones en la perseguibilidad de los delitos informáticos cometidos a través de Internet y se insiste en la necesaria colaboración judicial recíproca. Se menciona por vez primera la posición de vulnerabilidad en la que se encuentran ante este tipo de delitos -dadas las dificultades técnicas de su persecución- los países en vías de desarrollo y se urge a los países desarrollados a prestar su colaboración a aquellos. Nuevamente se expresa la necesidad de contar con una herramienta internacional de carácter imperativo para la protección contra la delincuencia informática, y se propone realizar un nuevo Convenio Internacional a semejanza del Convenio de 2001, aunque este extremo parece no contar con un consenso amplio ya que se señala que parece demasiado prematuro pues aún no existe una conclusión sobre los resultados y la eficacia de éste.

a.3. Otros instrumentos de Derecho Internacional.

a.3.1. La recomendación R(89)9 del Consejo de Europa.

Una de las herramientas que ha gozado de transcendencia internacional en cuanto a la regulación de los delitos informáticos ha sido la recomendación R(89)9 del Consejo de Europa[162]. En ella se reconoce la revolución que ha supuesto la implantación de las tecnologías de la información tanto en un sentido positivo como también en un sentido negativo, relativo a los abusos y el crimen derivado de la misma[163]. El texto de la recomendación, tras una introducción a la situación existente en la que repasa los trabajos de la OCDE (recordemos que la ONU no tratará esta materia hasta el 8º Congreso en 1990), procede a realizar un documento completo desde diversas perspectivas del delito informático.

La recomendación divide su contenido en cinco puntos fundamentales. El primero, en el que sitúa el fenómeno de la delincuencia informática en ese momento

[162] Recommendation nº R(89)9 of the Committee of Ministers to Member States on Computer-related Crime and Final Report of the European Committe on Crime Problems (aprobada por el Comité de Ministros el 13 de septiembre 1989 en la reunión 428 de Delegados), Ed. Council of Europe Publishing and Documentation Service, Estrasburgo, 1990.

[163] LEZERTUA RODRÍGUEZ, M.: "El Proyecto…" ob. cit. p. 89, destaca la labor del Consejo de Europa, al que se puede considerar "adelantado a su tiempo" y alaba el esfuerzo armonizador desde una temprana época de los delitos informáticos, siendo esta Recomendación muestra de ello.

histórico[164]. El segundo, en el que se centra en la elaboración de un listado sobre las conductas que deberían ser consideradas delictivas en los ordenamientos de los Estados; la novedad más significativa respecto del listado de la OCDE, y de los posteriores elaborados en esa época, es que hace una doble lista de conductas delictivas: en la primera de estas listas establece aquellas conductas que en todo caso deberían ser consideradas delictivas y, en una segunda lista, enumera una serie de supuestos de regulación recomendada[165]. Debemos recordar, una vez más, el carácter no vinculante de dicho documento, por lo que el ubicar las conductas merecedoras de reproche penal en una u otra lista, no tiene incidencia real en las políticas de los Estados que quieran regular los delitos informáticos. No obstante sí podemos extraer de este sistema de doble lista el hecho de reconocer una mayor preocupación por un tipo de conductas que por otras, y el priorizar los esfuerzos legislativos en las materias de la lista de mínimos. El tercer punto del texto trata sobre los problemas derivados de la persecución de estos delitos[166]. El cuarto punto señala problemas de jurisdicción y aplicación de la ley penal en el caso de los delitos informáticos al haber un componente de transnacionalidad en las conductas[167]. Sobre estos aspectos fue elaborada otra recomendación en 1995 relativa al mejor modo de actuar de los Estados para la persecución de estos delitos[168]. El quinto y último punto trata otros

[164] Recommendation nº R(89)9 on computer-related crime… ob. cit. pp. 9-32.

[165] En la Recommendation nº R(89)9 on computer-related crime… ob. cit. pp. 36-68, se reconocen dentro de la lista mínima el fraude informático, la falsificación informática, daños a datos o programas informáticos, el sabotaje informático, el acceso ilícito, la interceptación ilícita y delitos contra la propiedad intelectual e industrial. La lista opcional de conductas a regular incluye la alteración de datos o programas informáticos, el espionaje informático, la utilización de un ordenador sin consentimiento de su titular y la utilización de un programa informático sin el consentimiento de su titular.

[166] Recommendation nº R(89)9 on computer-related crime… ob. cit. pp. 69-82.

[167] Recommendation nº R(89)9 on computer-related crime… ob. cit. pp. 83-94.

[168] Recommendation nº R(95)13 of the Committee of Ministers to Member States Concerning Problems of Criminal Procedural Law Connected with Information Technology (aprobada por el Comité de Ministros el 11 de septiembre 1995 en la reunión 543 de Delegados), Ed. Council of Europe Publishing and Documentation Service, Estrasburgo, 1995. A ella se refiere LEZERTUA RODRÍGUEZ, M.: "El Proyecto…" ob. cit. pp. 91 y ss.

aspectos relacionados con la protección de las víctimas de delitos informáticos y los medios para prevenir éstos[169].

a.3.2. Las Conferencias Internacionales de la Universidad de Wurzburgo.

Entre el 5 y 8 de octubre de 1992 se celebraron tres conferencias internacionales en Wurzburgo, Alemania, organizadas por la Universidad de esta ciudad, centradas en la reunión y análisis de los datos relativos a la delincuencia informática en el mundo y cómo ésta había sido llevada a los ordenamiento penales de la mayor parte de países y cual era la hoja de ruta adecuada para los próximos años[170].

Estas tres conferencias corrieron a cargo de: 1) la Asociación Internacional de Derecho Penal (AIDP) sobre "delitos informáticos y otros delitos relacionados con las tecnologías de la información", 2) las Comunidades Europeas sobre "fraude informático y legislación sobre delincuencia informática en las Comunidades Europeas" y 3) la ONU respecto de "la contribución de las Naciones Unidas a la persecución y prevención de los delitos informáticos". Sobre el resultado final de las conferencias se puede decir que se realizó el estudio más denso y completo que se ha elaborado hasta la fecha, pues no sólo se hizo un repaso de la importancia creciente de los delitos informáticos, de su carácter trasnacional, y de las medidas que se están adoptando tanto por el Consejo de Europa, la ONU, y en menor medida, las Comunidades Europeas, sino que, además, gracias al trabajo de la AIDP, se analizan una por una las regulaciones penales que se han llevado a cabo en los ordenamientos jurídicos de más veinticinco países -incluido el análisis de España a principios de la década de 1990, a cuyas conclusiones nos referiremos más adelante[171]-.

---

[169] Recommendation nº R(89)9 on computer-related crime… ob. cit. pp. 94-104. Hace referencia a las mismas GUTIÉRREZ FRANCÉS, M. L.: "Reflexiones…" ob. cit. p. 83.

[170] SIEBER, U.: *Information Technology Crime. National Legislations and Internationals Initiatives*, Ed. Carl Heymanns Verlag, 1ª edición, Koln, 1994.

[171] Resultados de la misma publicados en AIDP: "Computer Crime and Other Crimes Againts Informátion Technology" en *Internacional Review of Penal Law*, Ed. Erès, nº 64, 1º y 2º trimestres, 1993, pp. 559-574, a cargo de GUTIÉRREZ FRANCÉS, M. L.

El resultado de las conferencias era, por tanto, una verdadera enciclopedia sobre la situación de la delincuencia informática en el mundo en la época[172] y, aún a pesar de tener el estatus de conferencias universitarias, las investigaciones allí puestas en común se convertirían en un material de trabajo fundamental para las investigaciones y propuestas en torno a la delincuencia informática en la siguiente década[173].

a.3.3. II Jornadas Internacionales sobre el Delito Cibernético.

Bajo la organización de la Universidad Nacional de Educación a Distancia de España (UNED) y el recientemente creado Grupo de Delitos Informáticos de la Guardia Civil[174], se celebraron en Mérida, España, del 20 al 22 de noviembre de 1997 las II Jornadas Internacionales sobre el Delito Cibernético[175].

En ellas se contó con la participación de numerosos especialistas, no sólo del ámbito jurídico sino también policial y político, del panorama nacional e internacional. Se trataron algunos de los temas mas relevantes de carácter general[176], y algunos especialmente relacionados con la denominada delincuencia informática a

[172] AIDP: "Computer…" ob. cit. p. 13.

[173] Especialmente relevante para los trabajos de la ONU tanto en su Manual publicado en 1994, como para los posteriores Congresos sobre prevención del delito y tratamiento del delincuente. También, aunque no se cita explícitamente en los trabajos legislativos de los Estados, se puede encontrar cierta relación entre la publicación de los trabajos de las conferencias y un nuevo impulso legislativo de los Estados para armonizar sus regulaciones penales, siendo el caso español paradigma de ello.

[174] Actualmente denominado Grupo de Delitos Telemáticos, se crea en el año 1996 ante las nuevas necesidades de contar con grupos de especialistas con conocimientos en informática y telecomunicaciones para desarrollar las investigaciones relacionadas con los abusos de sistemas informáticos. Inicialmente se denominó "Grupo de Delitos Informáticos" y posteriormente "Departamento de Delitos de Alta Tecnología". Desde el año 2003 se designó con el nombre "Grupo de Delitos Telemáticos" (GDT).

[175] Véase monográfico de sobre las "Jornadas Internacionales sobre el Delito Cibernético" en *Informática y derecho. Revista iberoamericana de derecho informático*, nº 27, 28 y 29, 1998.

[176] RIBAS ALEJANDRO, J.: "La sociedad digital: riesgos y oportunidades" en *Informática y derecho. Revista iberoamericana de derecho informático*, nº 27, 28 y 29, 1998, pp. 51 y ss., BENEDITO AGRAMUNT, J.: "Hacia la sociedad de la información" en *Informática y derecho. Revista iberoamericana de derecho informático*, nº 27, 28 y 29, 1998, pp. 233 y ss. o CARRASCOSA LÓPEZ, V.: "¿Es necesaria una legislación mundial para Internet?" en *Informática y derecho. Revista iberoamericana de derecho informático*, nº 27, 28 y 29, 1998, pp. 161 y ss.

través de Internet[177], pero también sobre el papel que las Fuerzas y Cuerpos de Seguridad del Estado debían ocupar en ese nueva estructura de persecución del delito informático transfronterizo[178] y otras temáticas ya clásicas en materia de delincuencia informática, como los daños informáticos o la protección de la intimidad[179].

Por lo demás, las Jornadas suponían la cada vez mayor implantación de una conciencia global sobre la necesidad de regular de forma adecuada el ámbito de las nuevas tecnologías no sólo en el ámbito administrativo o mercantil sino también en el penal, jurisdiccional o policial. Se puede afirmar que el tiempo entre la implantación de Internet y los sistemas informáticos personales, y la concienciación de la necesidad de un adecuado marco regulatorio fue muy breve; otra cosa es el tiempo en que esa conciencia global se ha traducido en una regulación penal adecuada e igualmente global.

[177] OVILLA BUENO, R.: "Algunas reflexiones jurídicas en torno al fenómeno Internet" en *Informática y derecho. Revista iberoamericana de derecho informático*, nº 27, 28 y 29, 1998, pp. 443 y ss., SÁNCHEZ BRAVO, A. A.: "La regulación de los contenidos ilícitos y nocivos en Internet" en *Informática y derecho. Revista iberoamericana de derecho informático*, nº 27, 28 y 29, 1998, pp. 361 y ss. o JAN DRIJBER, B.: "Enfoque común hacia el crimen organizado: el caso de la Unión Europea" en *Informática y derecho. Revista iberoamericana de derecho informático*, nº 27, 28 y 29, 1998, pp. 123 y ss.

[178] ATKINS, T.B.: "La cooperación internacional policial en el ciberespacio" en *Informática y derecho. Revista iberoamericana de derecho informático*, nº 27, 28 y 29, 1998, pp. 277 y ss. o MORAL TORRES, A.: "Colaboración policial internacional en el ciberespacio" en *Informática y derecho. Revista iberoamericana de derecho informático*, nº 27, 28 y 29, 1998, 353 y ss.

[179] ESTRADA POSADA, R. y SOMELLERA, R.: "Delitos informáticos" en *Informática y derecho. Revista iberoamericana de derecho informático*, nº 27, 28 y 29, 1998, pp. 423 y ss. También TÉLLEZ VALDÉS, J.: "Delitos cibernéticos" en *Informática y derecho. Revista iberoamericana de derecho informático*, nº 27, 28 y 29, 1998, pp. 113 y ss. Además, PIACENZA, D.F.: "Delitos informáticos" en *AR: Revista de Derecho Informático*, nº 127, 2009, (sin numerar), señala que se "ha creado una enorme brecha entre los países subdesarrollados y los países informatizados, por lo cual es lógico que en estos últimos se haya planteado primeramente este asunto de gran importancia".

B) REGULACIONES DE ÁMBITO NACIONAL EN PAÍSES DE NUESTRO ENTORNO

b.1) Estados Unidos, primer país en tener una regulación de ámbito estatal.

El origen de una protección amplia contra los delitos informáticos ha tenido su punto de partida desde una perspectiva de política legislativa nacional, como en la mayoría de los casos cuando nos movemos en el campo de la informática y las telecomunicaciones, en el Derecho penal estadounidense[180].

Haciendo un repaso cronológico de cómo ha tratado la legislación estadounidense los delitos informáticos debemos tomar como punto de partida la aprobación la *Counterfeit Access Device and Abuse Act* en 1984. Hasta este momento la persecución de las conductas en este ámbito se recogía en leyes estatales de aplicación limitada[181]. Es interesante para nuestro estudio al menos señalar, sin profundizar sobre esta cuestión, que la primera condena en Estados Unidos por realizar actos concretos de daños informáticos sobre sistemas ajenos fue resultado del procedimiento penal del Estado de Texas (que al igual que otros Estados recogía algunas prácticas delictivas sobre sistemas informáticos) contra Donald Gene Burleson en 1988. En dicho procedimiento se condenó al acusado por introducirse sin autorización y borrar datos de los ordenadores de la empresa de la que había sido

[180] Cabría matizar esta afirmación sobre la base de lo referido en SIEBER, U.: *The International…* ob. cit. p. 42, en la que se referencia que la primera regulación nacional a este respecto, aunque sumamente incompleta, se da en Suecia en 1973 que ya preveía algunos tipos penales relacionados con la protección de datos computerizados.

[181] En España es notable la recopilación de legislación de los Estados Unidos y la clasificación que en base a ésta realiza GUTIÉRREZ FRANCÉS, M. L.: *Fraude Informático y Estafa*, Ed. Ministerio de Justicia, 1ª edición, Madrid, 1991, pp. 123 y ss. Hace una división entre diferentes tipos de delitos informáticos: financieros, sustracción de información, y de acceso y uso no autorizado. En el mismo sentido BAKER, G. D.: "Trespassers Will Be Prosecuted: Computer Crime in the 1990s" en *Computer Law Journal*, nº 12, 1993, pp. 61 y ss. y NIMMER, R. T.: *Law of Computer Technology*, Ed. Thomson Reuters, 4ª edición, Nueva York, 2012, vol. 4, cap. 18. En general se utilizaban regulaciones sobre delitos en las comunicaciones o contra el patrimonio en las que se fueron añadiendo acciones en las que participaban ordenadores.

despedido en 1985, a una pena de siete años de libertad condicional y al pago de 11.800 dólares a la empresa afectada en concepto de responsabilidad civil[182].

Por tanto, la ley Federal *Counterfeit Access Device and Abuse Act* de 1984 supone un hito en la regulación penal de los abusos informáticos, no sólo en Estados Unidos, sino en el mundo, al ser la primera legislación de carácter nacional que se centraba directamente en la persecución de este tipo de acciones. Promulgada el 12 de octubre de 1984, establece diferentes delitos federales a partir del título "fraude y actividades relacionadas en la conexión entre ordenadores" para enjuiciar la actividad criminal informática[183]. Poco después de su entrada en vigor se descubrió como una herramienta trascendental, pero insuficiente -como se pudo observar al no poder ser aplicada en el caso de Donald Gene Burleson por no verse comprometidos los sistemas informáticos objeto de protección de la ley, que respondían a una lista cerrada y muy limitada- debido a lo cual pronto se prepararon enmiendas a la misma[184].

La enmienda aprobada en 1986 suponía entre otras cosas el cambio de nombre de la ley, que pasaba a denominarse *Computer Fraud and Abuse Act*[185] nombre por el cual se la conoce hoy en día. Con su aprobación y entrada en vigor se pretende tener una herramienta legal general para combatir el ataque a sistemas informáticos y hacer frente a los delitos federales cometidos por medios

[182] Información extraída de la sentencia de apelación referenciada como "Donald Gene Burleson, appellant v. The State of Texas, State nº 2-88-301-CR. Court of appeals of Texas, Second District, Fort Worth 802 S.W.2d 429; 1991 Tex. App. LEXIS 229. January 25, 1991", y del artículo "*Programmer Convicted After Planting a Virus*" publicado en el *NY Times* el 21 de septiembre de 1988.

[183] Referencia legal Pub. L. Nº 98-473.

[184] La *Counterfeit Access Device and Abuse Act* de 1984 se centraba en la persecución de tres tipos de actos delictivos que pronto se vieron superados por la realidad: acceso no autorizado a información del gobierno relacionada con la defensa nacional o las relaciones exteriores, acceso no autorizado a la información de las instituciones financieras y acceso no autorizado a la información general de los ordenadores del gobierno. La regulación por tanto obviaba los abusos que pudieran producirse sobre particulares o empresas privadas de cualquier ámbito. GUTIÉRREZ FRANCÉS, M. L.: *Fraude…* ob. cit. pp. 147 y ss. También ADAMS, J. M.: "Controlling Cyberspace: Applying the Computer Fraud and Abuse Act to the Internet" en *Santa Clara Computer & High Technology Law Journal*, vol. 12, nº 2, 1996, pp. 420 y ss.

[185] Referencia legal Pub. L. Nº 99-474.

informáticos. Es decir, su ámbito de aplicación se generalizaba y ampliaba respecto de la ley de 1984.

Bajo esta nueva regulación legal se produce en 1991 el primer gran juicio por la comisión de un delito federal de daños informáticos en Estados Unidos[186]. En el caso Estados Unidos contra Robert Tappam Morris se condenó al procesado por introducir un virus en la incipiente red de Internet en 1986 que provocó el colapso de diversos sistemas informáticos que vieron interrumpido su normal funcionamiento, sin que finalmente se produjesen daños sobre la información de los mismos, exceptuando el tiempo de inutilización de estos[187]. Entre otras cuestiones es interesante la sentencia del caso por mencionarse por vez primera en una Corte nacional la existencia de Internet y la necesidad de mejorar la seguridad en la red; Robert Tappam Morris fue condenado a tres años de libertad condicional, 400 horas de servicio comunitario y una multa de 10.050 dólares[188].

Esta ley ha sido nuevamente modificada por diferentes enmiendas. Concretamente en aquellas aprobadas en los años 1988, 1989 y 1990 se introdujeron algunas precisiones técnicas[189]. En las enmiendas de 1994, 1996, 2001, 2002 y 2007 se ampliaron los sistemas que iban a estar protegidos y se endurecieron las penas, además se incorporaron algunos conceptos derivados del Derecho Internacional que, en general, tratan de adaptar todo lo posible la regulación al momento actual y hacer cumplir los diferentes convenios de seguridad en la red suscritos por los Estados Unidos[190]. Aunque, como puede apreciarse, esta ley se ha visto reformada a través de la introducción de enmiendas -de forma constante- a lo largo de los años, son las

[186] Otros casos importantes en los Estados Unidos se pueden ver en CLOUGH, B. y MUNGO, P.: *Los piratas…* ob. cit. pp. 95 y ss.

[187] United States v. Morris, 928 F.2d 504, 505 (2d Cir. 1991).

[188] RUSTAD, M. L. y D'ANGELO, D.: "The path of Internet law: an annotated guide to legal landmarks" en *Duke Law & Technology Review*, nº 12, 2011: http://scholarship.law.duke.edu/cgi/viewcontent.cgi?Article=1226&context=dltr

[189] BEST, R. A. y PICQUET. C.: *Computer Law and Software Protection: A Bibliography of Crime, Liability, Abuse and Security, 1984 trought 1992*. Ed. Mcfarland, 1ª edición, Londres, 1993, p. 169 y ss.

[190] El más importante el Convenio sobre la Ciberdelincuencia de Budapest de 23 de noviembre de 2001 de cuyo análisis nos ocuparemos más adelante.

reformas de 1996 mediante la *Economic Espionage Act*[191] y la de 2001, a través de la reconocida *USA Patriot Act*[192], las dos modificaciones que han sido más importantes, tanto por su carácter expansivo como por la introducción de una cada vez más detallada tipología de conductas, de sanciones y de procedimientos de acción[193]. De tal forma que a través de esta regulación normativa queda configurada la protección sobre los denominados *Computer Crimes*, delitos cometidos mediante, o contra, ordenadores o dispositivos informáticos en general, véase telefonía móvil y cualquier otro tipo de equipo similar[194].

El caso más importante visto por los tribunales norteamericanos ha sido el denominado Estados Unidos contra David Lee Smith en 2002 por crear y distribuir el

[191] Referencia legal Pub. L. Nº 104-294, KELLY, D. J. y MASTROCOLA, P. R.: "The Economic Espionage Act of 1996" en *New England journal on criminal and civil confinement*, nº 26, 2000, pp. 181 y ss.

[192] Referencia legal Pub. L. Nº 107-56. Aprobada tras los atentados del 11 de septiembre de 2001 en Nueva York introducía numerosas reformas relacionadas con el ciberterrorismo y el recorte de ciertas libertades civiles para mejorar la seguridad nacional. Sobre el particular véase SKIBELL, R.: "Cybercrimes & misdemeanors: a reevaluation of the Computer Fraud and Abuse Act" en *Berkeley Technology Law Journal*, nº 18, 2003, pp. 908 y ss. Para una visión crítica: MELL, P.: "Big Brother at the Door: Balancing National Security with Privacy Under the USA Patriot Act" en *Denver University Law Review*, nº 80, 2002, pp. 375 y ss. Para una visión positiva de esta reforma: KERR, O. S.: "Internet surveillance law after the USA patriot Act: the big brother that isn't" en *Northwestern University Law Review*, nº 97, 2003, pp. 607 y ss.

[193] La actual regulación establece siete tipos de delitos informáticos incluyendo la punibilidad tanto de la consumación cómo de la tentativa: 1. Obtener información de seguridad nacional poniendo en peligro su confidencialidad, 2. Entrar sin autorización en un ordenador del gobierno, 3. Acceder sin autorización a un ordenador de una institución financiera o cualquier otro sistema protegido, 4. acceder a sistemas con la intención de defraudar para enriquecerse, 5. Dañar un ordenador o la información de éste, 6. Traficar con contraseñas, y 7. Amenazar con dañar un ordenador; en ELTRINGHAM, S.: *Prosecuting Computer Crimes*, Ed. US Department of Justice, 1ª edición, Washington DC, 2007, p. 2.

[194] Aunque no es un tema central en esta investigación, llama notablemente la atención si se compara con la realidad española, como el Departamento de Justicia de Estados Unidos subsume bajo la misma Sección los delitos informáticos y las infracciones contra la propiedad intelectual (*Computer Crime & Intellectual Property Section. United States Department of Justice)*, lo que parece expresar la preocupación que despierta la vulneración de los derechos de propiedad intelectual. La conclusión que se desprende de tal subsunción de tipologías bajo la misma Sección del Departamento de Justicia, más allá de la importancia que suscita en el Gobierno estadounidense, es que en la actualidad la mayoría de vulneraciones contra la propiedad intelectual se producen a través, o interrelacionadas de forma directa con los sistemas informáticos y las redes de comunicaciones. Además, la ley federal incorpora otro tipo de figuras delictivas en las que participan sistemas informáticos pero que, al menos en el ordenamiento español, no pueden ser consideradas delitos informáticos *stricto sensu*; hablamos de delitos de acoso a través de sistemas informáticos, delitos de robo de patentes a través de ordenadores o conspiraciones para delinquir a través de la red.

virus Melissa en Internet[195], virus que afectaba a archivos de Microsoft Office a través de la ejecución de un macro y con un sistema de distribución en Internet de virus gusano en 1999. Provocó el mayor caso conocido de infección masiva en la historia. No solo provocó daños en cientos de miles de sistemas informáticos en todo el planeta (dañaba todos los documentos de texto, hojas de calculo, presentaciones powerpoint, etc. del paquete Office de Microsoft), sino que también obligó a la paralización de la mayoría de empresas del mundo, incluidas muchas de las más importantes como Intel o Microsoft. David Lee Smith fue condenado a 10 años de cárcel, de los que cumplió 20 meses, y fue multado con 5.000 dólares[196].

En la actualidad destaca, en Estados Unidos, la cantidad de agencias y otras instituciones publicas y privadas que han aparecido, más allá de los textos legales, para dar forma de una u otra manera a la protección que la legislación trata de garantizar. El Instituto de Seguridad en Computadoras[197] (CSI) realiza informes anuales denominados "Estudios de Seguridad y Delitos Informáticos"[198] desde hace más de una década. Junto a esta organización de carácter privado se encuentra el interés del propio Gobierno estadounidense, y la institución del Centro de Quejas de Delitos por Internet[199] (IC3) que como ella misma se autodefine en su web oficial es una entidad gubernamental que establece la colaboración del FBI[200], el NW3C[201] y el

[195] La trascendencia de su afectación al concepto de seguridad en los sistemas de información se trata en MANSFIELD, R.: *Defensa contra hackers. Protección de información privada*, Ed. Anaya, 1ª edición, Madrid, 2001, pp. 265 y ss.

[196] Referencia de la sentencia: United States v. David Smith, Case Number 2:99-CR-730-01 (US District Court of New Jersey, 1999), DELTA, G. B. y MATSUURA, J. H.: *Law of the Internet*, Ed. Aspen Publishers, 2ª edición revisada, Nueva York, 2008, pp. 7 y ss. La trascendencia de dicho virus fue tal que provocó la inmediata respuesta de la Cámara de Representantes que inició estudios legislativos para tratar de mejorar la protección de los sistemas informáticos. Se pueden leer las intervenciones de los ponentes en VV.AA.: *The Melissa virus: inoculating our information technology from emerging threats: hearing before the Committee on Science, Subcommittee on Technology, U.S. House of Representatives, One Hundred Sixth Congress, first session, April 15, 1999*, Ed. U.S. Government Printing Office, 1ª edición, Washington DC, 1999.

[197] En inglés *Computer Secure Institute*. Organización estadounidense especializada en la seguridad en la red fundada en 1974.

[198] En inglés *Computer Crime and Security Survey*.

[199] En inglés *Internet Crime Complaint Center*.

[200] FBI son las siglas de *Federal Bureau of Investigation*, agencia estadounidense que se autodefine en su página web como organización de inteligencia cuya misión es defender y proteger los Estados Unidos contra amenazas de terrorismo y de inteligencia extranjeros, para defender y hacer

BJA[202] con el objetivo de servir como un vehículo para recibir, elaborar y remitir las denuncias penales teniendo en cuenta la rápida expansión de la delincuencia cibernética. El IC3 proporciona a las víctimas de los delitos cibernéticos un cómodo y fácil mecanismo de denuncia de actividades sospechosas relacionadas con internet, que alerta a las autoridades de presuntas violaciones penales o civiles.

b.2. Las primeras regulaciones a nivel estatal en Europa.

Al otro lado del océano, y con posterioridad, se sitúan las regulaciones de los Estados de la actual Unión Europea. En el viejo continente el primer país en regular esta materia fue la Republica Federal de Alemania en 1986, prácticamente al mismo tiempo que los Estados Unidos, que ya tipificaba, entre otras, las conductas de daños informáticos[203]. La necesidad de una nueva regulación sobre estas novedosas prácticas resultaba mucho más marcada en el caso alemán, pues la tradición penalista continental, que consagra el principio de legalidad penal como máxima inquebrantable no permitía, como había ocurrido en los Estados Unidos en un primer momento, incorporar las nuevas acciones en figuras anteriores ya reguladas con las que podrían guardar similitudes[204]. Así, gracias a la aprobación de esta ley, el

cumplir las leyes penales dentro de los Estados Unidos y prestar servicios de colaboración y ayuda penal a otras agencias federales, estatales, municipales y extranjeras.

[201] NW3C son las siglas de *National White Collar Crime Center*, que se autodefine como una corporación sin ánimo de lucro fundada por el Congreso de los Estados Unidos cuya misión es proporcionar colaboración y apoyo en investigación a los organismos y entidades implicadas en la prevención, investigación y enjuiciamiento de delitos económicos y de alta tecnología.

[202] BJA son las siglas de *Bureau of Justice Assistance*. Es un organismo dependiente de la Oficina de Programas Judiciales que se encuentra integrada en el Departamento de Justicia de los Estados Unidos.

[203] *Zweites Gesetz zur Bekampfung der Wirtschaftskriminalitat* (2.wikg) o Segunda Ley para la lucha contra la criminalidad económica, de 15 de mayo de 1986 que introducía en el StGB el espionaje de datos (§202.a), la estafa informática (§263.a) la falsificación de datos probatorios (§269) junto a modificaciones complementarias del resto de falsedades documentales como el engaño en el tráfico jurídico mediante la elaboración de datos, falsedad ideológica, uso de documentos falsos (§270, §271 y §273), la alteración de datos (§303.a), el sabotaje informático (§303.b) y la utilización abusiva de cheques o tarjetas de crédito (§266.b).

[204] GUTIÉRREZ FRANCÉS, M. L.: *Fraude…* ob. cit. p. 154, en realidad se refiere a la prohibición de analogía en el Derecho penal continental. Aunque en la actualidad la legislación penal de Estados Unidos de América recoge igualmente esta máxima, en ese momento no lo hacía con la misma intensidad que en los ordenamientos continentales (a partir de 1972 es cuando se comienza a plantear la idoneidad o no de que los jueces penales estadounidenses puedan crear Derecho). También ALTAVA

ordenamiento penal alemán pasa a regular acciones concernientes a la delincuencia informática como el espionaje de datos, la estafa mediante ordenador, el engaño en el tráfico jurídico mediante sistema de procesamiento de datos, la modificación no autorizada de datos y el sabotaje informático.

Siguiendo el modelo de su país vecino, Austria reforma su Código penal en 1987 para dar cabida a este tipo de conductas[205]. Francia en 1988 aprueba la Ley relativa al fraude informático[206] con ciertas peculiaridades respecto del resto de normas continentales ya que regulaba el fraude informático como una categoría especialmente amplia, en la que cabía casi cualquier ilícito en el que participase un ordenador[207]. Uno de los últimos países en afrontar la regulación general de este tipo de delitos fue el Reino Unido que en 1990 aprobó la ley sobre la materia[208]. Italia es el último de los principales Estados de Europa (exceptuando nuestro país, como veremos a continuación) en modificar su Código penal en las reformas de 1993 y de 1995 para tratar de dar acogida a una regulación penal adecuada de la mayor parte de conductas relacionas con el abuso de sistemas informáticos[209].

LAVALL, M. G.: *Lecciones de Derecho Comparado*, Ed. Universitat Jaume I, 1ª edición, Castellón de la Plana, 2003, pp. 255 y ss.

[205] La Ley de reforma del Código penal de 22 de diciembre de 1987 contemplaba por primera vez el daño sobre datos y programas informáticos (art. 126) y la estafa informática (art. 148).

[206] *Loi nº 88-19 du 5 janvier 1988 relative à la fraude informatique* o Ley 88-19 de 5 de enero de 1988 sobre el fraude informático, conocida como la Ley Godfrain tipificaba el acceso fraudulento a un sistema de elaboración de datos (art. 462.2), el sabotaje informático (art. 462.3), la destrucción de datos (art. 462.4), la falsificación de documentos informatizados (art. 462.5) y el uso de documentos informatizados falsos (art. 462.6). Se recomienda la lectura de DEVEZE, J.: "Commentaire de la Loi nº 88-19 du 5 janvier 1988 relative à la fraude informatique" en *Lamy droit de l'informatique*, nº febrero, 1988.

[207] DEVEZE, J.: "La fraude informatique, Aspects juridiques" en *La Semaine Juridique*, nº 3289, 1987, siguiendo la línea (previa a la aprobación de la ley) de JAEGER, M.: "La fraude informatique" en *Revue de Droit Penal et de Criminologie*, nº 65, 1985.

[208] *Computer Misuse Act* de 1990 o Ley de 1990 sobre el uso indebido de computadoras, en la que se regulaban exclusivamente tres conductas: el acceso ilegal a sistemas informáticos, el daño a los sistemas informáticos o a la información contenida en ellos, y realizar modificaciones de los sistemas informáticos sin autorización de su titular.

[209] Con la reforma del Código Penal del año 1993 se incluye expresamente la figura del fraude informático (art. 640 ter). En el año de 1995 se aprueba una nueva reforma del Código Penal en la que se regulan los daños informáticos (arts. 420 y 633) y se tipifica igualmente el acceso ilícito a datos contenidos en un sistema, red, o programa informático (art. 615 ter) y la detección y difusión abusiva de códigos de acceso a sistemas informáticos (art. 615 quarter).

El caso más importante de delincuencia informática en los primeros años de vigencia de estas recién estrenadas legislaciones penales se produjo en el Reino Unido en 1995. En 1990 Christopher Pile, también conocido como 'el Barón Negro' creó y distribuyó dos virus informáticos, ambos de muy difícil detección y con una capacidad destructiva considerablemente alta, pudiendo borrar toda información del disco duro de los sistemas informáticos infectados (virus de tipo polimórfico que distribuyó en diversos disquetes). Además, se procuró engañar a las víctimas introduciendo su *software* dentro de otros programas como juegos. Se estima que el virus causó daños por valor de un millón de libras esterlinas. Fue declarado culpable de once cargos en virtud de los artículos 2 y 3 de la *Computer Misuse Act* y condenado a una pena de prisión de 18 meses[210].

Tanto los casos conocidos por los tribunales norteamericanos, como el último ejemplo acaecido en el Reino Unido, no han sido los únicos durante los primeros años de las legislaciones penales de daños informáticos, pero sí tuvieron notable repercusión, y confirmaron la creencia original de que resultaba de vital importancia contar con unas herramientas legales adecuadas para estos casos. A partir de estas primeras condenas de la primera mitad de la década de 1990, coincidiendo con la implantación de los ordenadores personales y de Internet en las empresas, instituciones y hogares de los ciudadanos, el papel de estas regulaciones así como la repercusión de las sentencias dictadas con base en éstas supondrá un importante método de coacción para reprimir, en parte, el auge de la delincuencia informática. Se puede afirmar que había terminado la impunidad de los delincuentes informáticos[211].

[210] Artículo "*Mad boffin jailed over computer virus havoc*" publicado en *The Independent* el 16 de noviembre de 1995.

[211] Lo que de ninguna manera terminó con la delincuencia informática, que además lejos de disminuir ha ido aumentado progresivamente con la cada vez mayor implantación de la tecnología en la sociedad. Sin embargo, la importancia de contar con una regulación adecuada sí ha podido evitar de manera significativa que el campo de la informática se convierta en una suerte de mundo de anarquía en el que sólo el más fuerte podría estar seguro. Resulta interesante para comprobar tal afirmación el informe elaborado por Microsoft sobre *software malicioso en* 2012: http://www.microsoft.com/security/sir/story/#!10year

C) INTRODUCCIÓN A LA REGULACIÓN PENAL EN ESPAÑA

Con respecto al ordenamiento español, la regulación de la delincuencia informática hasta la aprobación del Código penal de 1995 era tremendamente insuficiente[212]. La jurisprudencia había dado cuenta de cierto tipo de fraudes electrónicos a través de la subsunción de ciertas conductas sancionándolas como apropiaciones indebidas[213], y la doctrina no tardó demasiado en hacer sus propuestas de interpretación[214] o regulación[215]. A esto debemos añadir que otras clases de delitos

[212] GUTIÉRREZ FRANCÉS, M. L.: "Computer Crime and Other Crimes against Information Technology in Spain" en AIDP: "Computer…" ob. cit. p. 574, señala que "en cuanto a la legislación en vigor nos gustaría expresar el hecho de que es completamente inadecuada en relación a la realidad de la nueva sociedad informatizada. La legislación sustantiva es insuficiente y la Ley de protección de datos es limitada". También GONZÁLEZ RUS, J. J.: "Protección penal de sistemas, elementos, datos, documentos y programas informáticos" en *Revista Electrónica de Ciencia Penal y Criminología*, nº 1, 1999, (edición electrónica sin numerar), señala que con el Código de 1995 "se pretende llenar las lagunas de punición que presentaba el Código penal anterior, en el que resultaban atípicos la mayor parte de los hechos de este tipo". MONTERDE FERRER, F.: "Especial consideración de los atentados por medios informáticos contra la intimidad y privacidad" en VELASCO NÚÑEZ, E. (dir.): *Delitos contra y a través de las nuevas tecnologías. ¿Cómo reducir su impunidad?*, Ed. Consejo General del Poder Judicial, Cuadernos de Derecho Judicial, 1ª edición, Madrid, 2006, pp. 196 y 197, añade que "a pesar de la mejor voluntad de los intérpretes escasamente podía contribuir [el anterior Código] a la tipificación y sanción penal de figuras criminales para las que no fue creado".

[213] FARALDO CABANA, P.: "Los conceptos de manipulación informática y artificio semejante en el delito de estafa informática" en *Eguzkilore: Cuaderno del Instituto Vasco de Criminología*, nº 21, 2007, p. 35, afirma que "en coherencia con la posición doctrinal mayoritaria, hasta la tipificación expresa de la estafa informática la jurisprudencia negaba que el fraude informático pudiera castigarse a través de la figura común de estafa. Es paradigmática la STS de 19-4-1991 (RJ 1991/2813), que revoca la sentencia de instancia, que castigaba por estafa y delito continuado de falsedad en documento mercantil al apoderado de una entidad financiera que, empleando alteraciones contables introducidas por medio del ordenador, consigue transferir y apropiarse de dinero de los clientes de la entidad, y, manteniendo la falsedad, castiga por apropiación indebida".

[214] Sobre el delito de daños GONZÁLEZ RUS, J. J.: "Tratamiento penal de los ilícitos patrimoniales relacionados con medios o procedimientos informáticos" en *Separata de Jornadas de estudio sobre nuevas formas de delincuencia*, 28 a 30 Noviembre 1988, pp. 12 y 13, sostiene que "estimo que la materialidad de la cosa debe ser entendida en sentido diverso de la aprehensibilidad que requieren los delitos de apoderamiento, debiendo insistirse en la capacidad del objeto [informático] para ser dañado o destruido". Realiza la misma reflexión en GONZÁLEZ RUS, J. J.: "Protección…" ob. cit. (sin numerar), "aunque ya en el Código anterior nada se oponía a la aplicación del delito a este tipo de elementos, con esta previsión el Código zanja la polémica en torno a la aplicación de los daños a los datos y elementos informáticos, negada para el Código anterior por la doctrina mayoritaria". También DE LA MATA BARRANCO, N. J.: "Utilización abusiva de cajeros automáticos: apropiación de dinero mediante la tarjeta sustraída a su titular" en *Poder Judicial* núm. nº IX (especial), 1988, pp. 172 y ss., propuso que la estafa no debía interpretarse estrictamente como una relación directa entre personas, sino que podían, al estilo de la autoría mediata, aparecen instrumentos -los sistemas informáticos- que llevasen a cabo ciertos elementos del tipo, sin que por ello, la relación defraudadora dejara de ocurrir.

vinculados directamente con la informática y tipificados en la actualidad como los relacionados con la intimidad o los daños no contaban con regulación penal alguna, teniendo que aplicarse, en los casos en los que era posible, interpretaciones extensivas de otros tipos sí recogidos, con las dificultades que eso plantea[216]. La conclusión es que el legislador español llegó con prácticamente una década de retraso al fenómeno informático respecto a los países de su entorno. Probablemente la justificación que se puede encontrar es que mientras los países más desarrollados pudieron entablar los procesos de modificación en los momentos de la aparición de estas nuevas conductas delictivas, la especialidad de la situación española, debida en parte a la transición política vivida en los últimos años de la década de los setenta, provocó que los mayores esfuerzos legislativos durante la década de los ochenta se centraran en materias de más inmediata necesidad, relegando las modificaciones pertinentes para dar cabida a estos nuevos tipos delictivos a un segundo plano, más si cabe cuando el Código penal vigente hasta mediados de los años noventa, el Código penal del 73, se había adaptado aceptablemente bien al nuevo marco Constitucional y

---

En una línea similar GUTIÉRREZ FRANCÉS, M. L.: "Delincuencia económica e informática en el nuevo Código Penal", en GALLARDO ORTIZ, M. A.: *Ámbito jurídico de las tecnologías de la información*, Ed. CGPJ, 1ª edición, Madrid, 1996, pp. 264-270.

[215] Notable es el trabajo de GUTIÉRREZ FRANCÉS, M. L.: *Fraude…* ob. cit., en el que pone en contraste la falta de regulación en España con la existente en otros países de nuestro entorno y expone la manera adaptar nuestra regulación construyendo lo que a su juicio deben ser nuevos tipos pensados para proteger nuevas situaciones que el Código penal vigente en esa época no era capaz de controlar. También realiza su propuesta en las Conferencias celebradas en Wuzburgo en 1992, GUTIÉRREZ FRANCÉS, M. L.: "Computer…" ob. cit. p. 574. Antes de estos trabajos resulta digno de elogio los resultados de las Jornadas sobre delincuencia económica organizadas por el Consejo General del Poder Judicial que se recogen en RUIZ VADILLO, E.: *Tratamiento de la delincuencia informática como una de las expresiones de la criminalidad económica*, Ed. Consejo General del Poder Judicial, 1ª edición, Madrid, 1988, en las que se recoge la problemática novedosa, la crítica sobre la falta de regulación en España y determinadas proposiciones al legislador para tipificar conductas informáticas indeseables (sobre modalidades comisivas, la autoría e incluso sobre la responsabilidad penal o cuasi penal de las personas jurídicas).

[216] Tales interpretaciones sobre delitos de revelación de secretos o daños se sugieren ya en 1988 en CORCOY BIDASOLO, M. y JOSHI JUBERT, U.: "Delitos contra el patrimonio cometidos por medios informáticos" en *Revista Jurídica de Catalunya*, vol. 87, nº 3, 1988, pp. 144 y ss. También se hace referencia en LANDA DURÁN, G. M.: "Los delitos informáticos en el Derecho penal de México y España" en *Revista del Instituto de la Judicatura Federal*, número 24, 2007, p. 246-249. En el mismo sentido LÓPEZ-VIDRIERO TEJEDOR, I.: *Delitos Informáticos ¿Cuáles son? ¿Cómo denunciarlos?* http://www.microsoft.com/business/smb/es-es/legal/delitos_informaticos.mspx

había dado cabida a importantes reformas necesarias tras la aparición de un Estado democrático y un régimen de libertad[217].

c.1. Los primeros casos de delincuencia informática en España.

Como hemos señalado en las líneas anteriores la regulación penal de los delitos informáticos en general era casi inexistente hasta la aprobación del Código penal de 1995. En todo caso, algunas figuras clásicas de la delincuencia informática si habían llegado a los tribunales, a través de la interpretación de los tipos penales ya existentes, generalmente las falsedades[218].

Los primeros procedimientos por delitos informáticos que gozaron de cierta trascendencia mediática y jurisdiccional en España no se dieron hasta la segunda mitad de la década de 1990 e incluso hasta ya entrado el año 2000; lo que una vez más demuestra el ritmo diferente de regulación y persecución que en nuestro país se ha realizado de este tipo de conductas. El primer juicio importante relacionado con delitos informáticos en España fue el derivado de la llamada Operación Toco, investigación llevada a cabo por la Guardia Civil en 1997. La labor del recién aparecido Grupo de Delitos Informáticos (GDI) de la Guardia Civil, (este caso supuso su primera investigación) permitió descubrir que dos sujetos -a la postre acusados- se matricularon en la Escuela de Ingeniería de la Universidad Rovira i Virgili de Tarragona en el curso 1996/1997 y desde allí, aprovechando la conexión de Internet, accedieron a las contraseñas de distintos usuarios de la red universitaria, entre ellas a las de más de 2.000 alumnos y de 150 de profesores de la universidad. Además accedieron a los sistemas del Centro de Supercomputación catalán y del Registro Mercantil de Tarragona. La fiscalía pidió tres años de cárcel para cada uno de ellos y una multa de 300.000 pesetas por la comisión de un delito de revelación de

[217] Entre otras modificaciones, destacan: la LO 2/1981 de 4 de mayo por la que se modifica el delito de rebelión y el de asociación ilícita, la LO 8/1983 de 25 de junio, de reforma urgente y parcial del Código Penal, que proclama definitivamente el principio de culpabilidad, actualiza la parte general en materias como el error o el delito continuado y modifica sustancialmente la parte especial, o la LO 7/1984 de 15 de octubre sobre tipificación penal de colocación ilegal de escuchas telefónicas.

[218] SSTS de 30 de noviembre de 1981, de 29 de noviembre de 1984 y de 5 de febrero de 1988, en las que se da entrada al documento electrónico por vía analógica. Sin embargo los fraudes informáticos difícilmente tenían cabida en el artículo 528 del Código de 1973 como señala GUTIÉRREZ FRANCÉS, M. L.: "Computer…" ob. cit. p. 568, no existiendo casos estudiados por la jurisprudencia.

secretos del artículo 197.1 y 197.2 del Código penal[219]. Cabe señalar que tanto la sentencia de instancia dictada por el Juzgado de lo penal nº 4 de Tarragona de 14 de julio de 2000 como la sentencia en apelación dictada por la sección 2ª de la Audiencia Provincial de Tarragona de 23 de julio de 2001, aceptaron como probados los hechos por los que se acusaba. Sin embargo, ambos acusados fueron finalmente absueltos. A pesar de haber cometido los hechos que se les imputaban, que pretendían insertarse en el tipo básico y agravado de revelación de secretos, lo cierto es que dichos tipos penales establecían unos requisitos típicos que excedían, en mucho, los hechos que realmente habían sido cometidos[220]. En efecto, la sentencia de apelación confirmaba que "no todo acceso irregular a datos ajenos ha de ser penalmente relevante ya que entonces los parámetros de aplicación del artículo 197 del Código Penal serían excesivamente amplios"[221], y concluye que por la prueba practicada, no se desprende la existencia de la intención de descubrir y desvelar secretos, sino tan sólo "la actitud de los acusados como un reto personal de obtener información sin fin"[222]. Por lo tanto, la conducta enjuiciada resultaba penalmente atípica[223].

Similares a los hechos anteriores son los descritos en la Sentencia del Juzgado de lo penal nº 2 de Barcelona de 28 de mayo de 1999, en los que se acusaba de un

[219] La redacción de los tipos penales del caso, a pesar de los años transcurridos no ha variado, sino que para completar las conductas típicas relacionadas con los delitos informáticos se han añadido nuevos apartados al citado artículo

[220] SAP de Tarragona, sección 2ª, de 23 de julio de 2001. El fundamento jurídico primero de la sentencia de apelación establece que los requisitos del tipo eran "a) un hecho de apoderamiento de datos, b) concurrencia de una voluntad de descubrir o conocer secretos o información privada ajena, c) que la indicada información privada o secretos ajenos tengan verdaderamente unas características de datos reservados u ocultos, d) que sean secretos de la persona o personas a que pertenezcan la titularidad de los datos reservados, y e) que en el apoderamiento, además del móvil inicial de conocer los secretos de otro u otros, concurra el *animus desvelandi o de divulgacion*, aunque no es indispensable, para la consumación del delito, que llegue a verificarse la susodicha divulgación."

[221] SAP de Tarragona, sección 2ª, de 23 de julio de 2001. F.J. 2, párrafo primero.

[222] SAP de Tarragona, sección 2ª, de 23 de julio de 2001. F.J. 2, párrafo tercero.

[223] Este caso guarda estrecha relación con otra causa que resultó finalmente archivada por el juez de instrucción. Así el Auto de 29 de enero de 2002 del Juzgado de instrucción nº 2 de Lorca archivó por no constituir delito el acceso ilegal a los ordenadores del Ministerio del Interior ocurrido en 1998, ya que no concurrían todos los elementos típicos previstos para el artículo 197.1 CP: "es por ello que las conductas de mero "*hacking*" acceso a los sistemas informáticos perpetrados con la única finalidad de acceder al *password* o puerta lógica no son actualmente constitutivos de delito pues carecen del elemento subjetivo del injusto".

delito de daños, previsto y penado en el art 264.2 del Código penal[224] al procesado. En dicha sentencia se declara probado el acceso no autorizado a los ordenadores de la Universidad Politécnica de Cataluña llegando a obtener privilegios de administrador instalando programas *sniffer*s destinados a capturar información que circula por la red[225], concretamente claves de acceso de otros usuarios sin que constara acreditado que el acusado participase en esa entrada ilegal a pesar de existir indicios sobre ello. En este caso la sentencia fue igualmente absolutoria, fundamentando tal fallo en que si bien los hechos podían ser constitutivos de delito, no se acreditaba suficientemente la participación en los hechos del acusado[226].

De los casos expuestos anteriormente se desprenden dos conclusiones. Por un lado, las primeras regulaciones de delitos informáticos tipificadas en España mediante el Código penal de 1995 eran sumamente imprecisas e incompletas. Y aún a pesar del avance que se estableció con el mismo, quedaban fuera de las acciones penales típicas algunos casos de acceso ilícito a sistemas informáticos o de daños informáticos[227]. Por otro lado, a pesar del perfeccionamiento de nuestra regulación penal, queda constancia de la dificultad de persecución de este tipo de delitos.

Por último, cabe señalar, incluyendo al caso español, que las diferentes regulaciones existentes en los países europeos o en Estados Unidos carecían de un nexo de unión y no parecían estar basadas en una política criminal concreta, ni mucho menos común, si bien no tendían a alejarse en exceso de las recomendaciones

[224] El artículo en cuestión fue profundamente reformado a través de la LO 5/2010 de 22 de junio. Hasta dicha reforma el tenor literal del artículo establecía que "la misma pena se impondrá [prisión de uno a tres años y multa de doce a veinticuatro meses] al que por cualquier medio destruya, altere, inutilice, o de cualquier otro modo dañe los datos, programas o documentos electrónicos ajenos contenidos en redes, soportes o sistemas informáticos".

[225] Véase capítulo primero.

[226] El denominado caso *Hispahack*, a él se refieren FERNÁNDEZ PALMA, R. y MORALES GARCÍA, O.: "El delito de daños informáticos y el caso *Hispahack*" en *La Ley. Revista Jurídica Española de Doctrina, Jurisprudencia y Legislación*, nº 1, 2000, pp. 1523 y ss.

[227] Extremo que en la actualidad ha sido superado con la aprobación de la LO 5/2010 de 22 de junio, que creando un nuevo apartado 3º del artículo 197 CP, establece como conducta prohibida el mero acceso a un sistema informático ajeno esquivando las medidas de seguridad de éste, suprimiendo por tanto el resto de requisitos de los apartados primero y segundo, especialmente el referido a la ánimo de descubrir y desvelar secretos; y también a través de una reformulación de los delitos de daños de los artículos 263 y 264 CP)

de los organismos internacionales. Mientras que en algunas regulaciones se introducían tipos exhaustivos y encargados de proteger diferentes bienes jurídicos, como era el caso alemán que regulaba la estafa, el espionaje, la alteración de datos o el sabotaje, otras regulaciones como la francesa, la británica o la española tipificaban sólo algunos de estos extremos. Sin embargo, el auge de este tipo de delitos, la progresiva sensibilización de los gobiernos de los Estados respecto de la gravedad de las conductas que lesionan bienes jurídicos supraindividuales, cometidas a través o contra medios electrónicos y, añadido a esto, el fenómeno globalizador focalizado en la cada vez más importante acción de la Unión Europea como un único interlocutor, organizador y en muchos aspectos regulador de importantes marcos legales, ha permitido el desarrollo de una política común y de colaboración entre los Estados y el avance significativo en la lucha contra estas prácticas.

3. CONVENIO SOBRE LA CIBERDELINCUENCIA DE BUDAPEST DE 23 DE NOVIEMBRE DE 2001

A) EL PREÁMBULO DEL CONVENIO Y EL CAPÍTULO PRIMERO

Desde una perspectiva internacional, la regulación imperativa en el ámbito penal para dotar a los sistemas normativos de los diferentes Estados de una armonización a nivel sancionador no se ha producido hasta un momento ciertamente tardío. Es en 2001 cuando el Consejo de Europa aprueba el texto del Convenio sobre la Ciberdelincuencia celebrado en Budapest[228], que es el primer instrumento internacional de carácter impositivo que pretende armonizar las diferentes legislaciones en materia penal relacionadas con los delitos informáticos[229]. Resulta importante señalar que los Estados Unidos de América, Canadá, Sudáfrica y Japón participaron en la elaboración y suscribieron dicho Convenio, además de los Estados miembros de la Unión Europea. Es, por tanto, y sin lugar a dudas, el instrumento internacional más importante, por su contenido y por el amplio consenso alcanzado,

[228] CHICHARRO LÁZARO, A.: "La labor legislativa del Consejo de Europa frente a la utilización de Internet con fines terroristas" en *Revista de Internet, derecho y política. Revista d'internet, dret i política*, nº 9, 2009, pp. 6 y ss. o SÁNCHEZ BRAVO, A. A.: "El Convenio…" ob. cit. pp. 6 y ss.

[229] Por todos DE LA CUESTA ARZAMENDI, J. L. y DE LA MATA BARRANCO, N. J.: *Derecho Penal Informático*, Ed. Thomson Reuters, 1ª edición, Navarra, 2010, p. 124.

aprobado en el seno de la Comunidad Internacional en relación con la materia que nos ocupa[230]. En todo caso es necesario matizar que las disposiciones que han sido aprobadas en dicho Convenio no son de aplicación directa, sino que su contenido sólo puede entenderse como la guía -impuesta- que deben seguir los Estados a la hora de elaborar sus normativas internas[231]. Esta necesidad de transposición queda expuesta en la redacción de su articulado, en la que se limita a llamar a los Estados adheridos al Convenio a acometer sus reformas, generalmente a través de la fórmula "cada Parte adoptará las medidas legislativas…". Aunque, como veremos, su implantación en la Comunidad Internacional se va produciendo poco a poco, su existencia es inestimablemente valiosa, y su capacidad para dar lugar a una protección adecuada se medirá en función del número de Estados por los que sea ratificado y aplicado[232].

El preámbulo del Convenio establece que, de continuidad con los tratados internacionales y convenciones ya existentes que tratan de armonizar la situación internacional en relación con el ámbito de la informática y las telecomunicaciones[233],

[230] Así lo establece la exposición de motivos de la Propuesta de Directiva del Parlamento Europeo y del Consejo relativa a los ataques contra los sistemas de información, por la que se pretende sustituir la Decisión Marco 2005/222/JAI del Consejo. "Está considerado [el Convenio de Budapest] como la normativa internacional más completa hasta la fecha, ya que establece un marco global y coherente que abarca los diversos aspectos de la ciberdelincuencia."

[231] MORILLAS CUEVA, L. y CRUZ BLANCA, M. J.: "Informática y delito. Aspectos penales relacionados con las nuevas tecnologías*"* en BENÍTEZ ORTÚZAR, I. F.: *Reformas del Código Penal. Respuestas para una sociedad del Siglo XXI,* Ed. Dykinson, 1ª edición, Madrid, 2009, p. 114.

[232] PÉREZ GIL, J.: "Medidas de investigación y de aseguramiento de la prueba en el Convenio sobre el cibercrimen" en VVAA: *Libro homenaje al profesor Dr. D. Eduardo Serra Font. Tomo II*, Ed. Ministerio de Justicia, Centro de Estudios Jurídicos, 1ª edición, Madrid, 2004, p. 1806, con acierto señala que "el carácter transfronterizo o desterritorializado predicable de muchas de las manifestaciones de la delincuencia que se sirve de sistemas informáticos nos viene a hablar de que cualquier medida normativa que no sea de carácter universal contiene vías de escape". También SÁNCHEZ SISCART, J. M.: "Cibercrimen…" ob. cit. pp. 32 y ss.

[233] Se mencionan expresamente entre otros el Convenio del Consejo de Europa de 1981 para la protección de las personas con respecto al tratamiento informatizado de datos personales, la Recomendación del Comité de Ministros R(85)10 relativa a la aplicación práctica del Convenio europeo de asistencia judicial en materia penal en relación con las comisiones rogatorias para la vigilancia de las telecomunicaciones, la Recomendación R(88)2 sobre medidas encaminadas a luchar contra la piratería en materia de propiedad intelectual y derechos afines, la Recomendación R(95)4 sobre la protección de los datos personales en el ámbito de los servicios de telecomunicaciones, con especial referencia a los servicios telefónicos; o el Plan de Acción adoptado por los Jefes de Estado y de Gobierno del Consejo de Europa con ocasión de su Segunda Cumbre para buscar respuestas comunes ante el desarrollo de las nuevas tecnologías de la información, basadas en las normas y los

surge la "necesidad de aplicar, con carácter prioritario, una política penal común encaminada a proteger a la sociedad frente a la ciberdelincuencia, entre otras formas, mediante la adopción de la legislación adecuada y el fomento de la cooperación internacional"[234], siendo por tanto la novedad con respecto a las anteriores regulaciones de origen internacional la pretensión de conseguir una armonización en el ámbito penal desde un punto de vista de política legislativa proveniente de un órgano de naturaleza supranacional, pero a diferencia de los instrumentos ya analizados, con un carácter netamente imperativo. El Convenio contiene un primer capítulo muy breve en el que se encarga de definir una serie de conceptos, de forma que sienta las bases de una terminología común para todos los Estados, procediendo en su capítulo segundo a establecer las guías para la regulación que los Estados deben realizar a nivel de derecho penal sustantivo, derecho procesal y de jurisdicción. Finalmente encontramos un tercer capítulo dedicado a los procedimientos de cooperación internacional en la materia. Además, su cuarto y último capítulo está dedicado exclusivamente a regular extremos tales como la aprobación, formas de adhesión y firma, denuncias, enmiendas, reservas etc.

Por su trascendencia en el posterior estudio del fenómeno de los daños informáticos vamos a centrar la disertación en la sección primera del capítulo segundo de este Convenio, donde aparecen las prácticas que se recomienda que deben ser tenidas en cuenta como conductas típicas en las legislaciones penales de los Estados adheridos en los artículos referidos a los daños informáticos. También señalaremos algunos apuntes sobre los aspectos procesales y de jurisdicción del resto del texto del Convenio De igual modo veremos las notas características del capítulo dedicado a la cooperación internacional en materia de persecución de delitos informáticos[235], así como la actual situación respecto de la adhesión de Estados al mismo.

---

valores del Consejo de Europa (celebrada los días 10 y 11 de octubre de 1997 en la ciudad de Estrasburgo).

[234] Preámbulo del Convenio sobre la Ciberdelincuencia de Budapest, de 23 de noviembre de 2001.

[235] FOGGETTI, N.: "Análisis de un supuesto de delincuencia informática trasnacional" en *Novática. Revista de la Asociación de Técnicos de Informática*, nº 166, 2003, p. 47. Se puede ver una síntesis para una idea general en RODRÍGUEZ BERNAL, A.: "España: Los Cibercrímenes en el Espacio de Libertad, Seguridad y Justicia" en *AR: Revista de Derecho Informático*, nº 103, 2007, pp. 12 y ss.

B) CAPÍTULO SEGUNDO

b.1. Sección primera. Derecho penal sustantivo.

Una primera aproximación al contenido de esta sección del Convenio permite apreciar cómo el legislador internacional ha decidido agrupar en cuatro títulos las conductas que deben ser sancionadas: a) delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos, b) delitos informáticos, c) delitos relacionados con la pornografía infantil y, finalmente, d) delitos relacionados con infracciones de la propiedad intelectual y derechos afines[236].

El título primero señala bajo la rúbrica de delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos las acciones de acceso ilícito -artículo 2-, interceptación ilícita -artículo 3- (vinculados a la acceso no autorizado a sistemas de comunicación y transmisiones electrónicas), interferencia de datos -artículo 4-, interceptación en el sistema -artículo 5- y el abuso de dispositivos -artículo 6-. En lo que a nuestra investigación interesará en la parte segunda, debemos centrar el estudio en el artículo 4 y el artículo 5 donde se puede observar cómo el Convenio trata de armonizar las cuestiones referentes a los daños informáticos[237].

El artículo 4.1 establece que "cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno la comisión deliberada e ilegítima de actos que dañen, borren, deterioren, alteren o supriman datos informáticos". Tal como queda redactado este apartado primero, se configura un delito que exige la causación de un resultado concreto para poder apreciarse (dañar, borrar, deteriorar, alterar o suprimir). Además, el legislador internacional reconoce en su apartado segundo capacidad a los Estados para que decidan si exigen, además de esas conductas, que el tipo penal sólo sea aplicable

[236] Sobre el Proyecto del Convenio se puede ver, LEZERTUA RODRÍGUEZ, M.: "El Proyecto…" ob. cit. pp. 95 y ss., cuyas investigaciones son esencialmente válidas para el texto finalmente aprobado.

[237] MORALES GARCÍA, O.: "Apuntes de política criminal en el contexto tecnológico. Una aproximación a la convención del Consejo de Europa sobre Cyber-Crime" en *Cuadernos de derecho judicial*, nº 9, 2002, pp. 29 y ss.

cuando con ellas se produzca un resultado grave, sin especificar parámetros con los que interpretar dicha gravedad.

Por otro lado, el artículo 5 establece que "cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno la obstaculización grave, deliberada e ilegítima del funcionamiento de un sistema informático mediante la introducción, transmisión, provocación de daños, borrado, deterioro, alteración o supresión de datos informáticos". En este segundo caso se regula otro tipo de daño informático, relacionado con la interferencia de sistemas informáticos. En el mismo sentido que el anterior, parece que el mandato al legislador nacional interpela a regular aquellas situaciones en las que se produzca un resultado concreto -la obstaculización-, que además deberá tener el carácter de grave. En realidad, la finalidad de las dos conductas recogidas en el Convenio es sancionar penalmente aquellas conductas graves -ya sea de daño a datos informáticos o de obstaculización de sistemas-. Sin embargo, la técnica legislativa utilizada es bien diferente. Mientras en el primer caso se redacta el supuesto sin mencionar la gravedad del resultado, y luego se habilita al legislador nacional a que, si lo desea, lo contemple sólo cuando el resultado sea grave, en el supuesto segundo, el Convenio sólo expresa la imposición de la regulación de la conducta cuando sea grave, lo que en realidad, habilita igualmente al legislador nacional a regular dicha acción en todos los supuestos, y no sólo los más graves. Más allá de lo ya apuntado cabe realizar ciertas reflexiones. En primer lugar, en cuanto a la tipificación de las acciones que son de interés desde la perspectiva penal, se observa la inclusión conjunta de dos conductas con elementos similares. Esto parece darnos a entender que, si bien son acciones diferentes, la protección recae sobre elementos esencialmente idénticos, esto es, la defensa de la propiedad de ciertos bienes inmateriales. Es decir, se regulan los daños en sentido amplio, si bien divididos en dos vertientes distintas. La del artículo 4, en la que se sanciona el mero daño sobre un determinado bien del sujeto pasivo; y la del artículo 5, en que la sanción va referida al perjuicio producido por la imposibilidad de utilización de un objeto, en este caso, un sistema informático en su conjunto[238].

[238] DE LA CUESTA ARZAMENDI, J. L. y DE LA MATA BARRANCO, N. J.: *Derecho…* ob. cit. p. 129.

Cabe añadir a lo referido anteriormente que el Convenio establece la necesidad de sancionar penalmente el abuso de los dispositivos, es decir, la producción, venta, obtención, importación o difusión de dispositivos o programas informáticos diseñados para la comisión de los delitos anteriores, así como de contraseñas o códigos de acceso a datos informáticos que permitan tener acceso a sistemas informáticos para perpetrar alguna de las acciones delictivas de los artículos anteriores (artículos 2 al 5 del Convenio)[239]. Visto este artículo, sorprende ver como en nuestro ordenamiento penal no se ha cumplido la exigida tipificación de estas conductas, más aun cuando España, pudiendo haberlo hecho, no ha formulado ninguna reserva al respecto. Por ello, cuando nos detengamos en la parte tercera de esta investigación en la proposición de un marco legal adecuado, volveremos sobre esta cuestión y realizaremos una propuesta de tipificación al respecto.

La sección dedicada al Derecho sustantivo continua con el título segundo que, bajo la rúbrica de delitos informáticos, aúna las acciones de falsificación informática -artículo 7- y fraude informático -artículo 8-, el título tercero se centra en los 'delitos relacionados con el contenido' informático, en el que exclusivamente señala conductas relacionadas con la pornografía infantil -artículo 9- y el título cuarto recoge los delitos relacionados con infracciones de la propiedad intelectual y de los derechos afines. Por último, existe un quinto título que trata las formas de comisión y la responsabilidad de las personas jurídicas, que no siempre tendrá porque ser de carácter penal[240]. También se recoge en este quinto título los requisitos que deben

[239] Es cierto que se señalan en el propio texto del Convenio algunas concreciones sobre la tipificación del abuso de dispositivos. Por un lado se da libertad a los legisladores nacionales para que establezcan un número determinado de elementos para la comisión de los actos delictivos a la hora de tipificar la conducta (art. 6.1.b). Además establece la posibilidad de formular reserva para la no aplicación de este artículo 6, excepto en lo referido a la distribución o cualquier otra puesta a disposición de una contraseña, un código de acceso o datos informáticos similares que permitan tener acceso a la totalidad o a una parte de un sistema informático (art. 6.3).

[240] Se salva así el inconveniente que supone, en algunas regulaciones de los Estados Parte, presentes o futuros, la inexistencia de responsabilidad penal de las personas jurídicas en sus ordenamientos. Véase por ejemplo el caso de España en el momento de elaboración del Convenio (no así en la actualidad). Sobre estos aspectos véase SILVA SÁNCHEZ, J. M.: "La responsabilidad penal de las personas jurídicas en el Convenio del Consejo de Europa sobre cibercriminalidad" en *Cuadernos de derecho judicial*, nº 9, 2002, pp. 115 y ss. Es cierto, en todo caso, que en la actualidad prácticamente todos los Estados de nuestro entorno tipifican la responsabilidad penal de las personas jurídicas en sus ordenamientos jurídicos, tanto en Europa como en Iberoamérica, siendo notables excepciones las de Alemania, Grecia e Italia con matices, ZUGALDÍA ESPINAR, J. M.: *La*

cumplir las sanciones que se establezcan en las diferentes regulaciones internas para dar cumplimiento a lo dispuesto en el Convenio[241]. Se exige la tipificación en los derechos internos de los Estados de la complicidad para los delitos de los artículos anteriores. Por el contrario, el Convenio es más laxo en cuanto a la tipicidad de la tentativa, ya que si bien recomienda que se adopte al menos respecto de los delitos de interceptación ilícita, interferencia de datos, interferencia en el sistema, falsificación informática, fraude informático, producción de pornografía infantil con vistas a su difusión y la difusión de pornografía infantil por medio de sistemas informáticos (artículos 3, 4, 5, 7, 8 y 9.1.a y 9.1.c), no lo exige de forma taxativa como se desprende de la cláusula del artículo 11.3 en la que establece la libertad los Estados de aplicar este extremo.

b.2. Sección segunda y tercera. Derecho procesal y jurisdicción.

Del artículo 14 al artículo 22, el Convenio detalla normas de carácter procesal y de jurisdicción[242]. Se parte, al igual que en la mayoría de los casos de los delitos tipificados en la sección primera, de la obligación de los Estados de incorporar a su regulación procesal los procedimientos y especialidades que se especifican en esta sección. En todo caso realiza un llamamiento a la protección adecuada de los derechos humanos y de las libertades de los individuos en función de otros Convenios existentes[243].

---

responsabilidad criminal de las personas jurídicas, de los entes sin personalidad y de sus directivos, Ed. Tirant lo Blanch, 1ª edición, Valencia, 2013, pp. 30 y ss.

[241] En realidad se produce un llamamiento a establecer sanciones tanto a personas jurídicas como autores individuales cumpliendo la exigencia mínima de ser proporcionales, efectivas y disuasorias, sin establecer en ningún caso su magnitud o alcance.

[242] El ámbito procesal se muestra estrechamente vinculado con el ámbito penal propio de esta investigación, por ello para una mayor profundidad en dicha materia en relación con el Convenio sobre la Ciberdelincuencia se recomienda PÉREZ GIL, J.: "Medidas…" ob. cit. pp. 1805-1847. También VELASCO NÚÑEZ, E.: "Cuestiones procesales relativas a la investigación de los delitos informáticos" en VELASCO NÚÑEZ, E. (dir.): *Delitos contra y a través de las nuevas tecnologías. ¿Cómo reducir su impunidad?*, Ed. Consejo General del Poder Judicial, Cuadernos de Derecho Judicial, 1ª edición, Madrid, 2006, pp. 309 y ss.

[243] Señala, concretamente en el artículo 15.1, el Convenio del Consejo de Europa para la protección de los derechos humanos y las libertades fundamentales (1950) y el Pacto Internacional de derechos civiles y políticos de las Naciones Unidas (1966)

Principalmente, los procedimientos establecidos (en las diferentes legislaciones procesales de los Estados Parte) suponen dotar de cierta uniformidad a la conservación rápida de datos informáticos -artículo 16-, la conservación y revelación parcial rápidas de datos sobre el tráfico -artículo 17-, la emisión de órdenes de comunicación e información emitidas por las autoridades -artículo 18-, el establecimiento de procedimientos similares y compatibles entre sí de registro y confiscación de datos informáticos almacenados -artículo 19-, de obtención en tiempo real de datos sobre el tráfico -artículo 20- y de interceptación de datos -artículo 21-.

C) CAPÍTULO TERCERO. COPERACIÓN INTERNACIONAL

Siguiendo las recomendaciones de todos los instrumentos internacionales relativos a la delincuencia informática que ya hemos analizado, el Convenio dedica su capítulo tercero a regular los métodos de cooperación internacional en la lucha contra la ciberdelincuencia, relacionándolo estrechamente con la sección segunda y tercera del capítulo segundo. Se trata, en definitiva, de mejorar las posibilidades de persecución y enjuiciamiento de los autores de los delitos señalados en la sección primera del capítulo segundo[244].

En realidad, el capítulo introduce pocas novedades destacables en cuanto los principios generales de cooperación -artículo 23- y de extradición -artículo 24-. Por un lado se establece que las Partes cooperarán entre sí en la mayor medida posible en aplicación de los instrumentos internacionales aplicables a la cooperación

[244] PÉREZ GIL, J.: "Medidas…" ob. cit. pp. 1815 y ss., desarrolla las normas procesales del Convenio, a la luz de la jurisprudencia del TEDH, en los ámbitos propios de éste, que serían: 1) el requerimiento de aportación o exhibición de datos informáticos, sobre el que, en su opinión, la doctrina del TEDH prima la protección del acusado y su derecho a no autoincriminarse, de tal forma que pueda rechazar el requerimiento de esos datos informáticos -no así cuando este requerimiento se dirija a un tercero en el proceso-; 2) el registro e incautación de sistemas y datos informáticos que no deben sino entenderse como medios de aseguramiento de la prueba, que responderán a las reglas comunes de registro e incautación de elementos del delito; y 3) la intervención de comunicaciones electrónicas sobre las que el TEDH ha insistido en la necesidad de establecer reglas claras y detalladas (STEDH, sección 3ª, de 25 de septiembre, caso P. G. y J. H. contra Reino Unido), en la línea de la doctrina sentada para las intervenciones telefónicas. En el ámbito doméstico y su acogimiento a la LECrim se puede consultar VELASCO NÚÑEZ, E.: "Aspectos procesales de la investigación y de la defensa en los delitos informáticos" en *Diario La Ley*, nº 6506, 2006, pp. 3 y ss.

internacional en materia penal, de los acuerdos basados en legislación uniforme o recíproca y de su derecho interno. Por otro lado, en cuanto a la extradición, establece las pautas generales de la misma siempre que sea por delitos cuya pena sea privativa de libertad por tiempo superior a un año, y siempre de forma supletoria a los tratados de extradición que puedan tener firmados al margen del Convenio las Partes implicadas y al Derecho interno de cada una de ellas. Además se regula la solución de controversias en materia de extradición.

En cambio, el Convenio enumera detalladamente los procedimientos y límites de la asistencia mutua en las labores de investigación y prevención -artículos 25 al 34- además de exhortar a los Estados que suscriban el Convenio a realizar las modificaciones legislativas necesarias para cumplir con dichas medidas[245]. Destaca la eliminación de trámites excesivamente burocráticos para la solicitud de asistencia (así, podrá bastar el envío de un e-mail entre las Partes para hacerlo en casos de urgencia). Además, en los casos relativos a solicitudes de asistencia mutua en ausencia de acuerdos internacionales en esta materia serán de aplicación obligatoria las disposiciones del presente Convenio. Los Estados Parte deberán designar a la autoridad central responsable de la asistencia mutua, que deberá velar por el cumplimiento tanto de las disposiciones del Convenio como de las de su derecho aplicable, para lo cual no podrá sobrepasar los límites impuestos en el propio Convenio[246], si bien en casos de urgencia podrá ser directamente la autoridad judicial la que recabe la asistencia. Igualmente se establecen unas pautas comunes sobre la conservación de datos informáticos almacenados en sistemas informáticos en los terminales situados en los Estados de alguna de las Partes para realizar labores de

[245] SÁNCHEZ SISCART, J. M.: "Cibercrimen…" ob. cit. pp. 33 y ss., clasifica las medidas que deben tomar los Estados y exhorta para regular en sus ordenamientos internos los siguientes extremos: a) preservación urgente de datos informáticos almacenados; b) revelación urgente de datos de tráfico almacenados; c) acceso a datos informáticos almacenados; d) acceso transfronterizo a datos almacenados, con consentimiento o cuando estén a disposición del público; e) asistencia mutua para la obtención en tiempo real de datos sobre el tráfico; f) asistencia mutua relativa a la interceptación en tiempo real de datos sobre el contenido; g) transmisión espontánea de información; y h) creación de red de puntos de contactos permanente denominados 'Red 24/7'.

[246] Básicamente las disposiciones del artículo 27.4 sobre denegación de asistencia (en general cuando se trate de delitos políticos o cuando la asistencia pueda atentar contra la soberanía, la seguridad, orden público u otros intereses esenciales), las del artículo 27.5 sobre suspensión de asistencia porque pueda causar perjuicios a otras investigaciones en marcha y las del artículo 27.8 y 28 sobre la solicitud de utilizar los datos facilitados en virtud de la asistencia de forma confidencial.

investigación. Pero más allá de lo anterior, también se estipula un instrumento de asistencia mutua de labores de investigación por el que una Parte podrá solicitar a las Fuerzas y Cuerpos de Seguridad de la otra que realice labores propias de la investigación de los delitos como si fuese la propia Parte interesada la que las realizase[247]. Cabe destacar, en la línea del nivel de detalle con que regula la asistencia mutua, por último, el establecimiento de la Red 24/7 -artículo 35- que como se desprende de su nombre supone un punto de contacto para la prestación de ayuda inmediata en orden a la realización de investigaciones relacionadas con los delitos informáticos que deberá encontrarse operativa en todo momento[248].

La existencia de este capítulo, aunque de difícil aplicación -o mejor dicho, de difícil aplicación eficaz- es fundamental para combatir el fenómeno de la delincuencia informática. La persecución de la delincuencia informática encuentra uno de sus mayores problemas en las dificultades de prevención del delito y normalmente la actuación de las autoridades judiciales y policiales opera una vez que se constata la producción de los resultados lesivos. Partiendo de este problema de difícil solución se hace, como mínimo necesario, articular un método eficaz de investigación y puesta a disposición de los autores de delitos informáticos entre los Estados para, en la medida de lo posible, si resulta del todo inalcanzable evitar sus ataques en primera instancia, sí lo sea impedir que estos se repitan[249].

[247] El artículo 31 del Convenio se refiere a las labores de entrada y registro y confiscación de sistemas y datos informáticos.

[248] Conforme establece SÁNCHEZ SISCART, J. M.: "Cibercrimen…" ob. cit. pp. 35, sus funciones principales serán: a) asesoramiento técnico; b) la conservación de datos en aplicación de los artículos 29 y 30; y c) la obtención de pruebas, el suministro de información jurídica y la localización de sospechosos.

[249] PÉREZ GIL, J.: "Medidas…" ob. cit. pp. 1846 y 1847, concluye que si bien la aprobación de dicho Convenio supone un hito tanto en el ámbito penal como procesal, por lo que respecta a este segundo, no debe ser coartada para "la invasión gubernamental en la esfera privada de los ciudadanos al margen del oportuno control jurisdiccional", mostrando a la vez su posición de reconocimiento ante tal instrumento y las dudas que le genera una aproximación excesiva al modelo norteamericano implantado por la *USA Patriot Act*, que superpone, en determinados ámbitos, la seguridad nacional a la privacidad personal. La misma preocupación expresa SÁNCHEZ BRAVO, A. A.: "El Convenio…" ob. cit. pp. 5 y 6.

D) CAPÍTULO CUARTO. DISPOSICIONES FINALES

El capítulo cuarto y último del Convenio -artículos 36 al 48- establece las clausulas generales que suelen acompañar a todo Convenio internacional: se establece que, en principio, el Convenio estará abierto a la firma de los Estados miembros del Consejo de Europa y de los Estados que sin ser miembros de éste participaron en su elaboración y que entrará en vigor el primer día del mes siguiente a la expiración de un plazo de tres meses desde que tres Estados miembros del Consejo de Europa y otros dos Estados (miembros o no) hayan expresado su consentimiento en quedar vinculados.

La apertura a firma se produjo en Budapest el mismo 23 de noviembre de 2001 y su entrada en vigor para los primeros Estados que expresaron su consentimiento se produjo el 1 de julio de 2004[250]. En la actualidad el Convenio ha sido ratificado por 37 Estados[251], y otros 10 Estados lo han suscrito pero no lo han ratificado todavía[252]. España firmó el Convenio el mismo día de la apertura a firma en 2001, pero no lo ha ratificado hasta el 3 de junio de 2010, entrando en vigor el 1 de octubre de ese mismo año[253]. Igualmente se establece que tras la entrada en vigor del Convenio el Comité de Ministros podrá, por unanimidad, invitar a otros Estados que no sean miembros del Consejo ni hayan participado en la elaboración del mismo a adherirse a éste, debiendo nuevamente aprobarse por unanimidad dicha adhesión.

Queda señalado igualmente que cuando dos o más Estados partes del Convenio ya tuvieran firmado, o lo hicieran en el futuro, otro Convenio en esta materia, el actual sólo regirá subsidiariamente, siempre y cuando las normas del

[250] Los primeros Estados en ratificar el Convenio fueron Albania el 20 de junio de 2002, Croacia el 17 de octubre de 2002, Estonia el 12 de mayo de 2003, Hungría el 4 de diciembre de 2003 y Lituania el 18 de marzo de 2004, todos ellos Estados miembros del Consejo de Europa.

[251] Albania, Armenia, Austria, Azerbaiyán, Bélgica, Bosnia y Herzegovina, Bulgaria, Croacia, Chipre, Dinamarca, Estonia, Finlandia, Francia, Georgia, Alemania, Hungría, Islandia, Italia, Letonia, Lituania, Malta, Moldavia, Montenegro, Holanda, Noruega, Portugal, Rumania, Serbia, Eslovaquia, Eslovenia, España, Suiza, Macedonia, Ucrania, Reino Unido, Japón y Estados Unidos de América.

[252] Canadá, Sudáfrica, Turquía, Suecia, Polonia, República Checa, Grecia, Irlanda, Liechtenstein, Luxemburgo,

[253] Aunque las reformas necesarias tras la ratificación del mismo no se convirtieron en una realidad en nuestro ordenamiento jurídico penal hasta la entrada en vigor de la LO 5/2010 de 22 de junio que se produjo el 24 de diciembre de 2010.

anterior no resulten incompatibles con las disposiciones de éste. Esta cláusula es importante, como veremos a continuación, respecto de los países pertenecientes a la Unión Europea, tras la aprobación Decisión Marco 2005/222/JAI de 24 de febrero, ya que limita, al menos en un sentido negativo, a ésta[254].

Los artículos 42 y 43 del Convenio establecen el marco de la formulación y retirada de reservas respecto de dicho Convenio, estableciendo una clausula cerrada respecto de las disposiciones sobre las que caben las reservas[255]. Como es habitual en este tipo de normas internacionales prácticamente todos los Estados han planteado reservas con mayor o menos intensidad[256]. España no ha formulado reservas al articulado del Convenio, si bien ha realizado tres declaraciones respecto al mismo de escasa trascendencia para nuestro estudio[257].

Aunque el texto del Convenio también establece el procedimiento para ser enmendado -artículo 44-, en la actualidad no se ha presentado ni aprobado ninguna enmienda sobre el mismo, por lo que su texto actual responde al elaborado en 2001. En lo que se refiere a los términos sobre cómo se encuentra regulada la solución de

[254] Es decir, la Decisión Marco podrá ampliar, limitar o matizar, para los Estados de la Unión Europea, las disposiciones del Convenio, pero en ningún caso redactar una norma incompatible con éste.

[255] Sólo podrán presentarse reservas en las materias recogidas en el apartado 2 del artículo 4, el apartado 3 del artículo 6, el apartado 4 del artículo 9, el apartado 3 del artículo 10, el apartado 3 del artículo 11, el apartado 3 del artículo 14, el apartado 2 del artículo 22, el apartado 4 del artículo 29 y el apartado 1 del artículo 41.

[256] Hasta 19 Estados han formulado reservas sobre alguno de los puntos permitidos.

[257] Declaración 1ª: Si la Convención se extendiera por el Reino Unido a Gibraltar, España desea formular la siguiente declaración: 1. Gibraltar es un territorio no autónomo cuyas relaciones internacionales están bajo la responsabilidad del Reino Unido y que está sometido a un proceso de descolonización de acuerdo con las decisiones y resoluciones pertinentes de la Asamblea General de las Naciones Unidas. 2. Las autoridades de Gibraltar tienen un carácter local y ejercen competencias exclusivamente internas que tienen su origen y su fundamento en la distribución y atribución de competencias efectuadas por el Reino Unido de conformidad con su legislación interna, en su calidad de Estado soberano del que el mencionado territorio no autónomo depende. 3. En consecuencia, la eventual participación de las autoridades gibraltareñas en la aplicación del presente Convenio se entenderá realizada exclusivamente en el marco de las competencias internas de Gibraltar y no puede ser considerado en modo alguno modificar lo establecido en los dos párrafos anteriores. Declaración 2ª: De conformidad con los artículos 24 y 27 de la Convención, España declara que la autoridad central designada es la Subdirección General de Cooperación Jurídica Internacional del Ministerio de Justicia. Declaración 3ª: De conformidad con el artículo 35 del Convenio, España declara que la autoridad central designada es la Comisaría General de Policía Judicial.

controversias, las consultas, las denuncias y las notificaciones no existen notas de especial relevancia para nuestro estudio.

E) PROTOCOLO SOBRE LA INCRIMINACIÓN DE ACTOS DE NATURALEZA RACISTA Y XENÓFOBA

Complementariamente a este Convenio de 2001 existe un Protocolo Adicional del año 2003 sobre la Incriminación de Actos de Naturaleza Racista y Xenófoba que viene a completar al anterior en cuanto a materias que habían quedado excluidas del mismo, pero que por razón de objeto estaban estrechamente vinculadas con la ciberdelincuencia de tal forma que trata de armonizar, con menos éxito que el anterior[258], la lucha contra el racismo y la xenofobia en los sistemas de información y las redes de comunicaciones e Internet. Aunque su vinculación con el estudio actual de los delitos informáticos en general es obvia, pues precisamente actos relacionados con motivos racistas o xenófobos pueden servirse igualmente de los sistemas informáticos para ser cometidos, creemos que profundizar en el contenido de este Protocolo resulta un asunto tangencial, de forma que no ahondaremos más en la cuestión[259].

[258] DE LA CUESTA ARZAMENDI, J. L. y DE LA MATA BARRANCO, N. J.: *Derecho…* ob. cit. pp. 134 y 135, señalan que "aunque es especialmente destacable el avance que, como complemento del Convenio de 2001, conlleva la adopción de este Protocolo, el mismo no completa la totalidad de conductas que debieran ser objeto de atención si se pretende una completa lucha contra lo que forma parte del concepto cibercrimen […] Pero es que además […] quedan extramuros del mismo aquellas otras [conductas], igualmente discriminatorias, de otra naturaleza (así, por ejemplo, en relación a supuestos de discriminación sexual o de discriminación motivada por deficiencias físicas o psíquicas)".

[259] Se recomienda para profundizar en el tema acudir al texto de PAVÓN PÉREZ, J. A.: "La labor del Consejo de Europa en la lucha contra la cibercriminalidad: El Protocolo Adicional al Convenio nº 185 sobre cibercriminalidad relativo a la incriminación de actos de naturaleza racista y xenófobos cometidos a través de los sistemas informáticos" en *Anuario de la Facultad de Derecho de la Universidad de Extremadura*, número 21, 2003.

4. MOVIMIENTOS REGULADORES EN EL ÁMBITO EUROPEO

A) DECISIÓN 92/242/CEE DEL CONSEJO, DE 31 DE MARZO, EN MATERIA DE SEGURIDAD DE LOS SISTEMAS DE INFORMACIÓN

El primer instrumento de la Unión Europea (entonces todavía Comunidad Económica Europea) en el marco de la seguridad informática se produce, en línea con los trabajos de otros organismos internacionales, a principios de la década de 1990. En concreto, mediante la Decisión 91/242/CEE del Consejo, de 31 de marzo de 1992, se adoptó una acción en el ámbito de la seguridad de los sistemas de información que incluía fundamentalmente dos elementos: a) el desarrollo de estrategias globales, o plan de acción, para la seguridad de los sistemas de información durante un periodo de 24 meses y b) la creación de un Comité de altos funcionarios que tendrá la misión a largo plazo de asesorar a la Comisión sobre acciones en materia de seguridad de los sistemas de información[260].

El plan de acción tenía como finalidad el desarrollo de estrategias globales destinadas a proporcionar a los usuarios y a los productores de información almacenada, procesada o transmitida electrónicamente la protección adecuada de los sistemas de información contra amenazas accidentales o deliberadas. Además, éste se ejecutaría en estrecha colaboración con los protagonistas del sector. Se debían tener en cuenta para el desarrollo del plan las actividades en curso a nivel mundial para la normalización en este ámbito[261]. Asimismo debía incluir las siguientes líneas de actuación: desarrollo de un marco estratégico para la seguridad de los sistemas de información, definición de las necesidades de los usuarios y de los prestadores de servicios en materia de seguridad de los sistemas de información, elaboración de soluciones para determinadas necesidades a corto y medio plazo de los usuarios, proveedores y prestadores de servicios, elaboración de especificaciones, normas y

[260] Artículo 1 de la Decisión 91/242/CEE del Consejo de 31 de marzo de 1992.

[261] Se ha señalado con antelación que a principios de la década de 1990 ya se habían puesto en marcha distintos instrumentos internacionales, principalmente recomendaciones, en las que se ponía de manifiesto la necesidad de unas políticas y unas regulaciones jurídicas adecuadas (OCDE, ONU, Consejo de Europa, etc.).

pruebas de certificación respecto a la seguridad de los sistemas de información, innovaciones técnicas y de funcionamiento en materia de seguridad de los sistemas de información en un marco estratégico general y, finalmente, la puesta en práctica de la seguridad de los sistemas de información. También se estipulaba que el Comité sería consultado sistemáticamente por la Comisión sobre los asuntos relacionados con la seguridad de los sistemas de información de las distintas actividades de la Comisión, en particular la definición de las estrategias y los programas de trabajo.

La primera reflexión que se extrae de la lectura de la Decisión de 1992 es que se constata por primera vez el interés real en el seno de la entonces Comunidad Económica Europea de armonizar y asegurar una evolución de las tecnologías de la información que garantizase la seguridad en la utilización de las mismas por parte de todos los sujetos de la Comunidad. Si bien queda patente en el texto de la Decisión, acorde con las competencias que la Comunidad Económica Europea ostentaba por aquel entonces, la ausencia de todo tipo de referencia al ámbito legislativo penal que debían seguir los Estados miembros. En efecto, ni el Tratado constitutivo de la Comunidad Económica Europea de 1957, ni las revisiones posteriores del mismo[262] otorgaron potestades en relación con la materia penal al organismo supranacional[263].

[262] A través, principalmente, del Tratado de Bruselas, denominado Tratado de fusión de 1965 (por el que se crea un Consejo y una Comisión únicos y se añade la constitución de un presupuesto de funcionamiento único); el Tratado que modifica algunas disposiciones presupuestarias de 1970 (por el que se sustituye al sistema de financiación de las Comunidades por contribuciones de los Estados miembros por el sistema de recursos propios y establece un presupuesto único para las Comunidades); el Tratado que modifica algunas disposiciones financieras de 1975 (por el que se otorga al Parlamento Europeo el derecho a rechazar el presupuesto y de aprobar la gestión de la Comisión en la ejecución del presupuesto e instituye un único Tribunal de Cuentas para las tres Comunidades); el Tratado de Groenlandia de 1984 (por el que se pone fin a la aplicación de los Tratados en el territorio de Groenlandia y establece relaciones especiales entre la Comunidad Europea y Groenlandia, iguales a las aplicadas a los Territorios de ultramar) y el Acta Única Europea de 1986 (por la que se realiza la primera gran reforma de los Tratados estableciendo la extensión de los casos de voto por mayoría cualificada en el Consejo, reforzando el papel del Parlamento Europeo y ampliando las competencias comunitarias).

[263] En realidad, ni el Tratado fundacional de la Comunidad Económica Europea de 1957 ni los posteriores especificaban la materia penal como una competencia propia, de lo cual se entendía que ésta quedaba excluida de sus potestades legislativas. Esta situación se mantiene hasta la Sentencia del Tribunal de Justicia de las Comunidades Europeas (STJCE) de 21 de septiembre 1989 en la que el Tribunal llegó a la conclusión de que, en orden a la protección de los intereses financieros de la Comunidad, las normas sancionadoras comunitarias no eran suficientes, de ahí la necesidad de que debían existir normas penales internacionales que establecieran tipos penales armonizados para perseguir conductas que afectaren a la debida protección de los intereses financieros de la Comunidad.

No aparece una competencia relativamente amplia para poder regular en este ámbito hasta el Tratado de la Unión Europa (Tratado de Maastricht), de 7 de febrero de 1992, cuando se introducen los principios de cooperación en el ámbito de justicia y asuntos de interior y, especialmente, hasta el Tratado de Ámsterdam de 1997, al consagrar el llamado espacio de libertad, seguridad y justicia[264].

Por lo tanto, no es de extrañar que la Decisión de la Comunidad Económica Europea en este sentido careciese de disposiciones directas referidas al Derecho penal de los Estados miembros, siendo su objeto, desde una perspectiva general, comenzar a realizar una observación activa del fenómeno de la delincuencia informática en el ámbito europeo y proveerse de órganos consultivos de expertos en la materia[265]. Dicho esto, es cierto que no se debe subestimar la importancia de esta Decisión desde un punto de vista de política común y de actuación de la Comunidad Económica Europea en materia de seguridad de los sistemas de información, por ser, precisamente, el primer instrumento relevante en el seno de la misma y por marcar el inicio de una preocupación constate de las instituciones europeas que no ha venido sino incrementándose desde entonces.

B) COM(2000)890 FINAL DE 26 DE ENERO DE 2001

Aunque se configura como un instrumento menor de la Unión, debemos referirnos, al menos brevemente, a la Comunicación de la Comisión al Consejo, al

[264] Véase CALONGE VELÁZQUEZ, A.: "Sistema competencial y de fuentes en el espacio de libertad, seguridad y justicia" en *Revista de derecho de la Unión Europea*, nº 10, 2006, pp. 95 y ss. En cuanto su perfil relacionado con los delitos informáticos véase RODRÍGUEZ BERNAL, A.: "España: Los Cibercrímenes…" ob. cit. pp. 23 y ss. A ello hace referencia BACIGALUPO SAGGESE, S.: "Derecho penal y construcción europea" en BACIGALUPO SAGGESE, S. y CANCIO MELIÁ, M. (coords.): *Derecho penal y política transnacional*, Ed. Atelier, 1ª edición, Barcelona, 2005, pp. 137 y ss., al señalar que a partir de la Constitución Europea se ha ampliado explícitamente el marco competencial en materia penal de la UE a delitos tales como terrorismo, trata de seres humanos o delincuencia informática entre otros.

[265] Dicha necesidad de personal cualificado, lejos de haberse podido superar, se ha intensificado con la evolución de la informática y las telecomunicaciones como se pone de manifiesto desde el propio sector, así FERNÁNDEZ FERNÁNDEZ, C.: "Delitos informáticos" en *Base Informática*, nº 43, 2009, p. 14, señala que "en la actualidad se precisa en muchos casos la presencia de la figura del perito, ya que hoy en día los ataques a través de la red, dirigidos a los Sistemas Informáticos, son cada vez más sofisticados debido a la facilidad de acceso a la información técnica que los Hacker tienen, en ocasiones utilizando Internet".

Parlamento Europeo, al Comité Económico y Social y al Comité de las Regiones sobre la creación de una sociedad de la información más segura mediante la mejora de la seguridad de las infraestructuras de información y la lucha contra los delitos informáticos, por ser el punto de partida fundamental de la regulación, ya sí en materia impositiva penal, que se ha desarrollado posteriormente en el seno de la Unión Europea.

En ella se señala que el desarrollo de las nuevas tecnologías de la información y la comunicación dieron lugar a importantes cambios, tanto desde una perspectiva económica como general, del modelo de funcionamiento de la sociedad. El éxito de la sociedad de la información es decisivo para el crecimiento, la competitividad y la creación de empleos en Europa y entre estos puntos destaca la importancia de la seguridad de las redes de comunicaciones y la lucha contra la, cada vez más instaurada, criminalidad informática. La creciente relevancia de las infraestructuras de información y comunicación ha abierto nuevas posibilidades a las conductas delictivas, lo que, entre otros programas, ha llevado a la Unión Europea a plantearse la aprobación de una serie de medidas iniciales en el marco de la estrategia de la Unión en materia de lucha contra la delincuencia que se sirve de las altas tecnologías.

La Comunicación define la delincuencia informática en un sentido amplio, como referido a "todo delito que implique la utilización de las tecnologías informáticas". Resuelve que los conceptos de delincuencia informática, delincuencia relacionada con la informática, delincuencia de alta tecnología y de delincuencia cibernética tienen el mismo significado en la medida que todos se refieren a: a) la explotación de las redes de información y comunicación sin ninguna dificultad geográfica y b) la circulación de datos intangibles y volátiles.

En la Comunicación se realiza un listado de los principales delitos que han sido introducidos en las legislaciones existentes[266] y se establecen una serie de

[266] Delitos contra la intimidad: recogida, almacenamiento, modificación, revelación o difusión ilegales de datos personales; delitos relativos al contenido: difusión, especialmente por Internet, de pornografía, y en especial de pornografía infantil, declaraciones racistas e información que incita a la violencia; delitos económicos, acceso no autorizado y sabotaje: muchos países han aprobado leyes que abordan los delitos económicos perpetrados por ordenador y tipifican nuevos delitos relacionados con el acceso no autorizado a sistemas informáticos (por ejemplo, la piratería, el sabotaje informático y la

propuestas de carácter legislativo y no legislativo que se deberán tomar en los años siguientes a la misma. Las medidas legislativas principalmente relacionadas con la armonización de las disposiciones nacionales en materia de delincuencia informática[267] deberían ser completadas mediante medidas no legislativas como la creación de unidades de persecución y prevención del delito nacionales especializadas, en las que se incluye la formación permanente y especializada de policías y personal de la administración de justicia, la creación de instrumentos adaptados para el análisis estadístico de la delincuencia informática y medidas de cooperación entre los distintos sujetos mediante la creación de un Foro europeo[268], además de fomentar acciones realizadas directamente por las empresas con el fin de luchar contra la delincuencia informática y realizar proyectos en el ámbito de la investigación y el desarrollo tecnológico con cargo a los presupuestos de la Unión Europea.

A partir de esta Comunicación, en la que ya se vislumbra la evolución de la política común, marcada por un aumento competencial de las materias en las que tiene potestades legislativas la actual Unión Europea, pero también en materias no propiamente legislativas como la cooperación e investigación, se produjeron, en el ordenamiento comunitario dos Decisiones Marco (una ya derogada por una Directiva de mayor alcance, y otra en vías de ser igualmente sustituida), relativas a la regulación en materia penal de delitos informáticos, cuyo contenido deriva en parte de la citada Comunicación[269].

---

distribución de virus, el espionaje informático, y la falsificación y el fraude informáticos); delitos contra la propiedad intelectual: delitos contra la protección jurídica de programas de ordenador y la protección jurídica de las bases de datos, los derechos de autor y derechos afines.

[267] La Comisión presentará propuestas legislativas en los siguientes ámbitos: armonización de las legislaciones de los Estados miembros en el ámbito de los delitos relativos a la pornografía infantil, armonización de los sistemas de derecho penal material en el ámbito de la delincuencia que se sirve de las altas tecnologías y aplicación del principio de reconocimiento mutuo relativo a las medidas cautelares previas a los pleitos vinculados a las investigaciones en materia de delincuencia informática que implican a más de un Estado miembro.

[268] Que reúna principalmente a las autoridades encargadas de la aplicación de las leyes, a los proveedores de servicio, operadores de redes, asociaciones de consumidores y autoridades encargadas de la protección de los datos con el fin de intensificar la cooperación a escala comunitaria.

[269] Esta línea se continua con la COM(2001)298 final, Bruselas, 6 de junio de 2001, Seguridad de las redes y de la información: Propuesta para un enfoque político europeo, en la que se tratan más

C) REGULACIÓN PENAL DE LA UNIÓN EUROPEA EN MATERIA DE DELITOS INFORMÁTICOS

c.1. Directiva 2011/93/UE del Parlamento Europeo y del Consejo, de 13 de diciembre de 2011.

Esta Directiva relativa a la lucha contra los abusos sexuales y la explotación sexual de los menores y la pornografía infantil viene a sustituir la Decisión Marco 2004/68/JAI del Consejo, de 22 de diciembre de 2003, sobre la misma materia, que fue la primera normativa europea que establecía tanto acciones típicas concretas como marcos penales abstractos y otra serie de medidas de ámbito penal y procesal en materia de delincuencia informática[270].

Se enuncian una serie de comportamientos que deben considerarse ilícitos en relación con "la lucha contra la explotación sexual de los niños y la pornografía infantil". Aunque se aleja del estudio propio de la segunda y tercera parte de esta investigación, es importante, y a eso dedicaremos las siguientes líneas, al menos señalar aquellas cuestiones de interés por tratarse, en definitiva, de una regulación penal supranacional de una parte de los llamados delitos informáticos en sentido amplio que realiza la Unión Europea.

En la línea con la Decisión Marco que deroga, comienza su articulado marcando el objeto de la misma en el artículo 1, para continuar con una serie de definiciones sobre lo que debe entenderse por menor, pornografía infantil, prostitución infantil, espectáculo pornográfico y persona jurídica; para, a partir de su artículo tercero, enumerar las conductas que los Estados deberán regular en sus ordenamientos penales. En el ámbito general de está investigación cabría destacar como acciones que quedan tipificadas la exposición de un menor a actos de carácter sexual -artículo 3.2- o a abusos sexuales -artículo 3.3-[271], asistir a espectáculos

---

concretamente algunos aspectos relativos a la seguridad en las redes y sistemas de información; para una visión general SÁNCHEZ BRAVO, A. A.: "Una política comunitaria de seguridad en Internet" en *Diario La Ley*, nº 5414, 2001, pp. 1 y ss.

[270] GALÁN MUÑOZ, A.: "La internacionalización…" ob. cit. p. 93.

[271] En los que, si bien no aparece explícitamente la utilización de los sistemas informáticos como medio para realizar estas exposiciones, bien podría ser un medio de cometer las acciones típicas.

pornográficos en los que participen menores -artículo 4.4-[272], la adquisición o la posesión de pornografía infantil, el acceso a sabiendas a pornografía infantil por medio de las tecnologías de la información y la comunicación, la distribución, difusión o transmisión de pornografía infantil, el ofrecimiento, suministro o puesta a disposición de pornografía infantil -artículo 5-, la propuesta por parte de un adulto, por medio de las tecnologías de la información y la comunicación, de encontrarse con un menor que no ha alcanzado la edad de consentimiento sexual con el fin de realizar actos de carácter sexual o de producir pornografía infantil -artículo 6-.

La Directiva insta a que se tipifique, acorde con los ordenamientos penales de los Estados, la inducción, la complicidad y la tentativa de, por lo menos, las acciones de los artículos 3 y 6 -artículo 7-. Se establece también un catálogo de circunstancias agravantes para las acciones anteriores, cuando éstas sean cometidas contra un menor en una situación de especial vulnerabilidad o que son cometidas por un miembro de la familia que conviva con el menor o por una persona que haya abusado de su posición reconocida de confianza o autoridad o por varias personas actuando conjuntamente o en el marco de una organización delictiva[273] o cuando el autor sea reincidente, haya puesta en peligro la vida del menor o se haya empleado violencia grave contra el menor causándole un daño grave -artículo 9-. Además, a fin de evitar el riesgo de reincidencia los Estados deberán adoptar las medidas necesarias para garantizar que una persona física que haya sido condenada por las acciones de los artículos 3 a 7 sea inhabilitada, al menos temporalmente, para el ejercicio de actividades profesionales que impliquen contactos directos y regulares con menores -artículo 10-.

En el ámbito procesal se estipulan otras medidas que los Estados miembros deben llevar a sus ordenamientos relacionadas con el embargo y decomiso -artículo

[272] En la misma línea que los casos anteriores, cabría preguntarse si una reunión para ver películas de pornografía infantil integraría la acción típica.

[273] Ya hemos señalado que si bien el estudio completo de las acciones típicas relativas a la pornografía infantil excede del ámbito de esta investigación, al menos se debe mencionar que los pocos casos de delitos informáticos en el marco de una organización delictiva que han llegado a ser conocidos por nuestro Tribunal Supremo han sido en relación a este tipo de conductas, VELASCO NÚÑEZ, E.: "Delitos informáticos realizados en actuación organizada" en *Diario La Ley*, nº 7743, 2011, (edición electrónica sin numerar), hace referencia a la STS de 10 de diciembre de 2004 (Maza Martín), con los matices críticos de la STS de 20 de septiembre de 2006 (Martín Pallín).

11-, la responsabilidad penal de las personas jurídicas -artículos 12 y 13- y otras medidas de carácter procesal, de esclarecimiento del delito, de asistencia a las víctimas y de prevención del delito -artículos 15 a 25-

Entre otras cuestiones destaca que la presente Directiva deroga la Decisión Marco de 2003 (artículo 26), que si bien regulaba el mismo ámbito, lo hacía de una forma menos extensa y menos concreta, de tal forma que en apenas 2 artículos recogía todo el elenco de acciones punibles[274]. Así mismo, la Decisión Marco derogaba la Acción Común 97/154/JAI, de 24 de febrero de 1997, adoptada por el Consejo sobre la base del artículo K.3 del Tratado de la Unión Europea, relativa a la lucha contra la trata de seres humanos y la explotación sexual de los niños -artículo 11- en la que, de una forma todavía mucho más laxa y general, impelía a los Estados

[274] En ella se insta a los Estados a tipificar en sus ordenamientos penales una serie de conductas relativas a la explotación sexual de menores y la pornografía infantil. En cuanto a la explotación sexual de menores establece la tipificación de conductas como la de coaccionar a un niño para que se prostituya, explotar o lucrarse con dicha prostitución o facilitarla por cualquier otro medio, practicar con un niño actividades sexuales recurriendo a la fuerza, la coacción o la amenaza, ofrecer dinero u otras formas de remuneración a cambio de servicios sexuales o abusar de una posición reconocida de confianza, autoridad o influencia sobre el niño. No obstante, esta parte, en la medida en que no aparecen los sistemas informáticos no es relevante para nuestro estudio -artículo 2-. En cambio, sí lo es aquella referida a los comportamientos punibles relacionados con la pornografía infantil que se realicen mediante sistemas informáticos tales como la producción de pornografía infantil, la distribución, difusión o transmisión de pornografía infantil, el ofrecimiento o facilitación por cualquier otro medio material de pornografía infantil y la adquisición o posesión de material de pornografía infantil -artículo 3-. Además insta a los Estados miembros a adoptar las medidas necesarias para garantizar la punibilidad de la inducción en las infracciones mencionadas, así como la tentativa de comisión de las mismas -artículo 4-. Las sanciones penales previstas por cada Estado deberían incluir una pena privativa de libertad de al menos entre uno y tres años y se tipificarían una serie de circunstancias agravantes que en caso de concurrir elevarían la pena a una duración al menos de cinco a diez años. Además, los Estados podrían introducir disposiciones destinadas a inhabilitar a las personas físicas, condenadas por una de las infracciones enunciadas, para el ejercicio de actividades que supongan el cuidado de niños -artículo 5-. La Decisión Marco introducía la responsabilidad de las personas jurídicas sin especificar una obligación sobre si esta debía ser penal, civil o administrativa, responsabilidad que es complementaria de la de la persona física y no sustituye por tanto a las personas que hayan cometido materialmente las acciones -artículos 6 y 7-. Además, la Decisión establecía las pautas para la resolución de controversias por conflicto de competencias introduciendo criterios de atribución así como cuestiones relacionadas con la protección y asistencia a las víctimas -artículos 8 y 9-. Por último, también se señalaba que los Estados deberían tomar las medidas necesarias para que en fecha de 20 de enero de 2006 sus ordenamientos jurídicos internos estuvieran adaptados a la presente Decisión Marco -artículo 12- y que se emitiese un informe sobre la implantación de la misma (Finalmente el Informe COM(2007)716 final, de 16 de noviembre de 2007, basado en el artículo 12 de la Decisión Marco 2004/68/JAI del Consejo, de 22 de diciembre de 2003, relativa a la lucha contra la explotación sexual de los niños y la pornografía infantil).

a regular penalmente acciones del mismo tipo que las recogidas en la actual Directiva[275]. Por último, de un modo similar al de su predecesora, establece como fecha máxima el 18 de diciembre de 2015 para la presentación al Parlamento Europeo de un informe elaborado por la Comisión sobre la implantación de la normativa en los ordenamientos jurídicos de los Estados miembros sin haber, en este caso, un límite temporal explícito para que los Estados incorporen a sus legislaciones dichas medidas -artículo 28-.

c.2. Decisión Marco 2005/222/JAI del Consejo, de 24 de febrero de 2005.

c.2.1. La Decisión Marco. Unificación de criterios.

Esta Decisión Marco tiene por objeto luchar contra la delincuencia informática y promover la seguridad de la información más allá de los delitos ya previstos en la derogada Decisión Marco 2004/68/JAI del Consejo, de 22 de diciembre de 2003, y en la actual Directiva 2011/93/UE del Parlamento Europeo y del Consejo, de 13 de diciembre de 2011, relativos -entre otras cuestiones- al uso de los sistemas informáticos en acciones relacionadas con la pornografía infantil. Frente a esta nueva forma de delincuencia transnacional, el principal objetivo es reforzar la cooperación tanto entre las autoridades judiciales como entre las Fuerzas y Cuerpos de Seguridad de los Estados miembros, mediante una armonización de sus normas penales, que reprima los ataques contra los sistemas de información de forma similar en todos países de la Unión Europea[276].

La Decisión Marco 2005/222/JAI, de 24 de febrero, establece en su artículo

[275] Con la entrada de en vigor del Tratado de Amsterdam de 1997 las Acciones Comunes en la cooperación policial y judicial en materia penal se ven sustituidas por las Directivas y Decisiones Marco, que gozan de mayor capacidad normativa, como se puede apreciar viendo el texto de la Decisión Marco 2004/68/JAI del Consejo, de 22 de diciembre de 2003 y la Acción Común 98/733/JAI, en las que, si bien ambas son de obligado cumplimiento para los Estados miembros, el texto de la Acción Común se limita a establecer las conductas y a solicitar que éstas tengan consideración de infracción penal, sin establecer marcos penales y otras herramientas de cooperación entre Estados, muy lejos del nivel de concreción alcanzo por la posterior Decisión Marco en la materia.

[276] HUETE NOGUERAS, J.: "La reforma de los delitos informáticos" en *Diario La Ley*, nº 7534, 2010, p. 2, señala que "destaca en la Exposición de Motivos de la propia Decisión Marco, la distancia y las divergencias significativas que existen entre las legislaciones de los Estados miembros". También RODRIGUEZ BERNAL, A.: "España: Los Cibercrímenes…" ob. cit. pp. 26 y ss.

primero una definición común para el concepto de "sistemas de información" que deben adoptar todos los Estados miembros, conforme a la cual se establece como sistema de información *"*todo aparato o grupo de aparatos interconectados o relacionados entre sí, uno o varios de los cuales realizan, mediante un programa, el tratamiento automático de datos informáticos, así como los datos informáticos almacenados, tratados, recuperados o transmitidos por estos últimos para su funcionamiento, utilización, protección y mantenimiento*".* Como ya se expuso en el capítulo primero, creemos que el término más adecuado debería ser el de sistema informático[277], sin embargo, la utilización de uno u otro, visto lo que ha entendido el legislador europeo por tal carece de importancia, al referirse, en realidad, a lo mismo.

Parece, en todo caso, que una vez más los pasos que sigue la regulación europea en todo aquello relacionado con la informática y las telecomunicaciones son los que ya se han seguido, implantado y aceptado como válidos en los Estados Unidos. Prueba de ello, y volviendo a la Decisión Marco 2005/222/JAI, es que la definición que nos aporta, por primera vez de manera común a todos los europeos, extrae, aunque con otra redacción, los mismos principios que marcan los estándares americanos[278] y que son los siguientes:

1. Equipo o grupo de equipos: la Decisión Marco establece como requisito de los sistemas de información que estén compuestos por lo menos de un terminal, aunque también establece que un grupo de terminales puede entenderse, por si solo como un sistema de información[279].

[277] Como de hecho fue utilizado en la Decisión Marco 2004/68/JAI del Consejo, de 22 de diciembre de 2003, relativa a la lucha contra la explotación sexual de los niños y la pornografía infantil.

[278] Ya se ha señalado en esta investigación que la definición elaborada por el *American National Standards Institute* entiende que un sistema de información es un "sistema o subsistema de telecomunicaciones o computacional interconectados y que se utilicen para obtener, almacenar, manipular, administrar, mover, controlar, desplegar, intercambiar, transmitir o recibir voz y/o datos, incluyéndose en el mismo tanto los programas (*software* y *firmware*) como el equipo (*hardware*)"

[279] Por ejemplo, un único ordenador de una oficina puede ser considerado como un sistema de información, pero igualmente todos los ordenadores de la oficina que están conectados en red pueden ser considerados en su conjunto como un solo sistema de información (formado por varios sistemas de información singulares)

2. Interconectados: esos diferentes equipos, o grupos de equipos tienen que estar conectados de alguna manera, o tener la capacidad de estarlo, lo que nos introduce en el campo de las redes de información, paradigma de las cuales es Internet.

3. Para el tratamiento de datos: ese sistema o grupo de sistemas permite trabajar con datos, dándole aquí a datos un significado informático amplio, en el que se consideran como tales voz, audio, imagen, etc. Además este tratamiento puede ser de muchos tipos: envío, recuperación, modificación, etc.

El resto del artículo primero de la Decisión Marco 2005/222/JAI de 24 de febrero, está dedicado a definir otros tres conceptos. El primero de ellos referido a los datos, en su sentido informático, no en cuanto a una información concreta sobre algo o alguien[280]. Cabe señalar de modo introductorio ahora, que un documento electrónico es la suma de varios -miles de- datos informáticos estructurados de una determinada forma que permiten su representación visual en un sistema informático. Exactamente de la misma manera se configura un programa informático, como la unión estructurada de miles de datos cuya representación visual sobre un sistema informático permite realizar diferentes funciones. Por todo ello, aunque la mención a programas informáticos o documentos electrónicos podría resultar aclaratoria, se puede entender que dichos conceptos quedan subsumidos en el más general de 'datos informáticos'. En este artículo primero también se define lo que debe entenderse por persona jurídica a los efectos de la Decisión Marco[281]. Y por último lo que ha de considerarse por falta de autorización[282]. Cuestiones en las que nos detendremos en detalle más adelante.

[280] Es importante no confundir el término dato informático, con dato en sentido general, como los que protege por ejemplo la Ley de protección de datos cuando en su artículo 3 define los datos como "información concerniente a personas físicas identificadas o identificables". No es correcto para estos supuestos.

[281] Será persona jurídica a efectos de la Decisión Marco "toda entidad a la cual el derecho vigente reconoce este estatuto, salvo los Estados y otros organismos públicos que ejercen prerrogativas estatales y las organizaciones internacionales de derecho público".

[282] Se entenderá sin autorización "el acceso o la intromisión no autorizados por el propietario o titular de otro tipo de derecho sobre el sistema o parte del mismo o no permitidos por la legislación nacional".

Tras este primer artículo, desde el artículo segundo al cuarto se establecen las conductas que son consideradas merecedoras de reproche penal y a partir de ahí la Decisión Marco se centra en otras cuestiones de tipo general, como el grado de participación en la acción típica -artículo 5-, las sanciones -artículo 6-, las circunstancias modificativas -artículo 7-, aspectos relacionados con las personas jurídicas -artículos 8 y 9- y otras cuestiones conexas.

c.2.2. Derecho penal sustantivo que impone la Decisión Marco.

En lo que a nuestra investigación interesa corresponde ahora analizar cómo ha tratado esta Decisión Marco la regulación de los daños informáticos y si sigue el camino marcado por el Convenio sobre la Ciberdelincuencia de Budapest de 2001 o si añade o suprime algún elemento que resulte interesante estudiar.

Se ha mencionado *supra* que los artículos segundo a cuarto son los que establecen las conductas que deben ser sancionadas por los Estados miembros de la Unión Europea. La redacción de la Decisión Marco establece tres categorías generales: acceso ilegal a los sistemas de información, intromisión ilegal en los sistemas de información e intromisión ilegal de datos. A este respecto, interesa ahora la figura de intromisión ilegal en los sistemas de información -artículo 3- y la intromisión ilegal de datos -artículo 4-. En lo que al acceso ilegal -artículo 2- se refiere, no es una regulación protectora de la integridad de los datos en relación con los daños que sobre ellos puedan recaer, sino que centra su protección en otro ámbito relacionado estrechamente con la intimidad o la inviolabilidad informática[283]; por lo que excede de los contornos de lo que a nuestra investigación ocupa.

Podemos comenzar señalando que el artículo 3 de la Decisión Marco regula la intromisión ilegal en los sistemas de información estableciendo que "cada Estado miembro adoptará las medidas necesarias para que el acto intencionado, cometido sin autorización, de obstaculizar o interrumpir de manera significativa el funcionamiento de un sistema de información, introduciendo, transmitiendo, dañando, borrando,

[283] En nuestro ordenamiento la exigencia de transposición del acceso ilegal ha sido ubicada en el artículo 197.3 CP, como un delito de descubrimiento y revelación de secretos. La expresión inviolabilidad informática es acuñada por GALÁN MUÑOZ, A.: "La internacionalización…" ob. cit. pp. 95 y ss.

deteriorando, alterando, suprimiendo o haciendo inaccesibles datos informáticos, sea sancionable como infracción penal, al menos en los casos que no sean de menor gravedad". El artículo 4 de la Decisión Marco regula la intromisión ilegal de datos, estableciendo que "cada Estado miembro adoptará las medidas necesarias para que el acto intencionado, cometido sin autorización, de borrar, dañar, deteriorar, alterar, suprimir o hacer inaccesibles datos informáticos contenidos en un sistema de información sea sancionable como infracción penal, al menos en los casos que no sean de menor gravedad"[284].

Cuestión que debe ser analizada es la derivada de comprobar si las conductas que se recogieron en su día en el Convenio y las conductas que han quedado recogidas ahora en la Decisión Marco resultan compatibles entre sí, pues no se debe olvidar que los Estados miembros de la Unión Europea, en la medida en que se han adherido a dicho Convenio, deben modificar sus ordenamientos penales en la línea por él marcada, pero tendrán igualmente que hacerlo en la línea establecida por la Decisión Marco. En ésta se exige reconocer como acciones penalmente sancionables tres conductas, en concreto tres de las cuatro primeras conductas que recoge el Convenio, quedando fuera la interceptación ilícita, cuestión en la que nos vamos a detener a continuación por su directa relación con las que sí han quedado tipificadas, y otras acciones con una naturaleza sustancialmente diferente[285].

Resulta complicado entender los motivos del legislador europeo a la hora de excluir esta cuarta acción ilícita de las demás. Pudiera ser que su fundamento a la hora de establecer la actual situación normativa se encontrara en que la Decisión Marco entiende que en la interceptación ilícita el bien jurídico protegido en sí mismo

[284] Una de las primeras cuestiones a mencionar, aunque seguramente no la más importante, respecto de la redacción de la Decisión Marco en referencia a la regulación del Convenio sobre la Ciberdelincuencia, es la decisión de intercambiar el orden numérico de los artículos de las conductas previstas. En efecto, la regulación proveniente del Convenio tipifica en primer lugar la interferencia de datos (lo que sería la intromisión ilegal de datos en la Decisión Marco con las salvedades que haremos más adelante), y en segundo lugar la interferencia del sistema (equivalente a la ahora intromisión ilegal en los sistemas de información de la Decisión Marco). Este orden ha sido invertido en la Decisión Marco, sin que exista motivo aparente para ello.

[285] Por tanto, han quedado excluidas de la Decisión Marco además de la interceptación ilícita, las conductas de abuso de dispositivos, falsificación informática, fraude informático, los delitos relacionados con la pornografía infantil y los relacionados con la propiedad intelectual.

no son los datos o los sistemas de información, sino el secreto de comunicaciones o la intimidad, bien jurídico ampliamente protegido en las regulaciones constitucionales y penales de los Estados miembros[286]. Por tanto, mientras que las conductas efectivamente tipificadas en la Decisión Marco tienden a proteger la integridad de los datos y de los sistemas de información como objetos de nuevo cuño merecedores de protección penal, la acción excluida protege unos intereses que, aunque relacionados intrínsecamente con la informática, no son exclusivos de ésta, sino más bien una modalidad de otro tipo de ilícitos ya regulados[287]. Cuestión distinta es la idoneidad o no de excluir de la Decisión Marco la interceptación ilícita recogida en el Convenio, que a diferencia del resto de conductas reguladas en el apuntado Convenio y excluidas aquí[288], si presenta unos rasgos homogéneos a los de las conductas tipificadas en la Decisión Marco. En primer lugar porque, como hemos dicho, aunque el bien jurídico puede ser sustancialmente diferente -si bien este extremo será discutido llegado el momento-, los medios comisivos son, en general, los mismos. Además, parece extraerse de la regulación del Convenio de 2001 que las cuatro acciones (intromisión ilegal y acceso ilegal en los sistemas de información, intromisión ilegal en los datos e interceptación ilícita) pretenden ser englobadas como una serie de conductas que, si bien ya podían encontrarse mejor o peor acomodadas en las regulaciones de los Estados firmantes en preceptos originariamente pensados para otras acciones delictivas[289], el legislador internacional

[286] DE ESTEBAN ALONSO, J. y GONZÁLEZ-TREVIJANO SÁNCHEZ, P.: *Tratado de Derecho Constitucional II*, Ed. Universidad Complutense Madrid, 2ª edición, Madrid, 2004, p. 137, señala que "el derecho al secreto de las comunicaciones engloba tanto el secreto tradicional de la correspondencia […] como cualquier otra forma de comunicación […] especialmente el correo electrónico". En el mismo sentido se expresan FERNÁNDEZ SANTIAGO, A. y CASTRO FUERTES, M.: "Comentario al artículo 197 CP" en AMADEO GADEA, S. (dir.): *Código Penal. Doctrina Jurisprudencial. Parte especial* Ed. Factum Libri Ediciones, Madrid, 2009:
http://0-vlex.com.cisne.sim.ucm.es/vid/comentario-articulo-codigo-penal-69108467

[287] Exactamente en nuestro Código penal en el artículo 197.1 se recoge de alguna manera la interceptación de emails y telecomunicaciones (entre otros) como constitutivos de delito cuando tienen por objeto vulnerar la intimidad o descubrir secretos. Aunque resulta importante señalar que su redacción es sustancialmente diferente a la ofrecida por el Convenio sobre la Ciberdelincuencia de Budapest de 2001.

[288] Conductas de abuso de dispositivos, falsificación informática, fraude informático, los delitos relacionados con la pornografía infantil y los relacionados con la propiedad intelectual.

[289] Véase por ejemplo la situación española, donde la regulación de los daños ya existía, y el hecho de cometerse con medios informáticos se consideraba como una circunstancia agravante del daño común, pero no como un tipo autónomo hasta la reforma de 2010.

ha querido dotarlas de una autonomía normativa que produjese su escisión de aquellas figuras delictivas dentro las cuales fueron originariamente englobadas. Autonomía, por tanto, que la Decisión Marco habría creado para las tres acciones incluidas en ella, pero como hemos señalado, autonomía de la que no ha considerado oportuno dotar a la interceptación ilícita, manteniendo por tanto en esta modalidad la sujeción que en los diferentes ordenamientos tenga a la inviolabilidad de las comunicaciones[290].

Pero es que además, y para finalizar este inciso, sobre la exclusión de esta acción parece estarse dando una nueva visión dentro de las instituciones europeas; en concreto el Parlamento Europeo y el Consejo, que han propuesto la aprobación de una nueva Directiva que derogue a la actual Decisión Marco, en la que en realidad se viene a completar la anterior e introducir nuevas conductas penalmente sancionables[291], además de algunas otras cuestiones que trataremos más adelante. Por tanto y como ya se ha señalado anteriormente, resulta difícil entender la exclusión de la interceptación en la todavía vigente Decisión Marco, más cuando la -muy probable y cercana- aprobación de la Directiva que la sustituya va a introducir dicha conducta, sumándola así al resto de las acciones anteriores, y copiando casi literalmente el texto de la regulación del Convenio de 2001.

[290] Como hemos mencionado, en la actual regulación del Código penal español, el artículo 197.1 sanciona acciones con un contenido similar al que establece el Convenio sobre la Ciberdelincuencia en relación con la interceptación ilícita pero sin autonomía propia respecto de otras figuras como la interceptación de papeles o cartas: " El que, para descubrir los secretos o vulnerar la intimidad de otro, sin su consentimiento, se apodere de sus papeles, cartas, mensajes de correo electrónico o cualesquiera otros documentos o efectos personales o intercepte sus telecomunicaciones o utilice artificios técnicos de escucha, transmisión, grabación o reproducción del sonido o de la imagen, o de cualquier otra señal de comunicación, será castigado con las penas de prisión de uno a cuatro años y multa de doce a veinticuatro meses".

[291] La propuesta de Directiva, aún en fase de aprobación, pero con amplio consenso para ser aprobada sin excesivas modificaciones, añade a las tres acciones que recoge la actual Decisión Marco, la de interceptación ilícita que reconocía el Convenio de Ciberdelincuencia.
Artículo 7 propuesto: "Los Estados miembros adoptarán las medidas necesarias para garantizar que la interceptación intencionada, por medios técnicos, de transmisiones no públicas de datos informáticos hacia, desde o dentro de un sistema de información, incluidas las emisiones electromagnéticas de un sistema de información que contenga dichos datos informáticos, se castigue como una infracción penal cuando se cometa sin autorización".

c.2.3. Otros extremos contenidos en la Decisión Marco.

Al margen de aquellos puntos relativos a la legislación penal, la Decisión Marco también establece algunas cuestiones relativas a la competencia para enjuiciar los delitos anteriores. Principalmente, se establece que los Estados deberán hacer las modificaciones legislativas necesarias para juzgar a los autores de estos delitos, aun cuando los efectos de sus acciones se hayan producido en otros Estados. Asimismo se regula la solución de controversias en esta materia -artículo 10-.

De forma análoga a como lo hacía el Convenio, la Decisión también establece la necesidad de regular unos procedimientos similares en los Estados de la Unión Europea para el intercambio de información, la creación de un punto de contacto 24/7, así como la designación de la administración que gestione dicho punto -artículo 11-.

Por último, cabe señalar que la propia Decisión Marco en su artículo 12 establece que los Estados miembros deberán haber adoptado las medidas necesarias en sus ordenamientos internos para dar cabida a las previsiones de la Decisión antes del 17 de marzo de 2007. Además, antes del 17 de septiembre de 2007 el Consejo de la UE evaluará en función del informe presentado por la Comisión en qué medida los Estados miembros han dado cumplimiento a las disposiciones de la presente Decisión Marco.

Habiendo trascurrido ya los plazos señalados en el mencionado artículo 12, podemos realizar algunas apreciaciones sobre el proceso actual de incorporación al Derecho interno de los Estados de la Decisión Marco. En primer lugar, cabría destacar que según el archivo del Consejo[292] respecto de las previsiones del artículo 12 no existe a día de hoy la evaluación del Consejo sobre la implantación de la normativa, aunque sí se elevó el Informe por parte de la Comisión[293]. En dicho informe, de fecha 14 de julio de 2008, la Comisión, tras enunciar los antecedentes de

[292] Consultado el 2 de enero de 2013.

[293] COM(2008)448 final, de 14 de julio de 2008. Informe de la Comisión al Consejo basado en el artículo 12 de la Decisión Marco del Consejo, de 24 de febrero de 2005, relativa a los ataques contra los sistemas de información.

dicho informe y los objetivos originarios de la Decisión Marco pasa a realizar la evaluación donde señala que en la fecha originalmente prevista para los Estados para informar de la situación de la aplicación de la Decisión Marco (16 de marzo de 2007) sólo Suecia había transmitido la forma de transposición a su ordenamiento a la Comisión. Vista la situación, se volvió a pedir a los Estados miembros que enviaran el texto de las disposiciones nacionales de transposición de la Decisión Marco, de tal modo que en fecha 1 de junio de 2008 veinte Estados miembros habían comunicado las reformas en sus ordenamientos penales, mientras que otros siete Estados miembros, entre los que se encontraba España, no habían cumplido la obligación de notificación que les impone el artículo 12, apartado 2, de la Decisión Marco. Es por tanto, a partir de la transposición de la normativa de esos veinte Estados cumplidores en torno a la cual se hace el informe.

Por lo que respecta a España, como ha venido ocurriendo reiteradamente en el ámbito de las nuevas tecnologías, no adaptó, como veremos, su legislación penal de forma acorde con el contenido de la Decisión Marco hasta la reforma operada por la LO 5/2010 de 22 de junio. Podríamos entender, por tanto, que no realizase comunicación alguna a la Comisión respecto de sus labores de transposición al ordenamiento de la Decisión Marco, excepto por el hecho, de que ya existía en nuestro país un proyecto de reforma del Código penal en tramitación parlamentaria en 2008, derivado de los trabajos realizados en la Comisión General de Codificación en los años 2005 y 2006 en los que ya se contemplaba la adaptación de nuestra legislación penal en materia de delitos informáticos a las imposiciones de la Unión Europea; lo que en nuestra opinión hubiese merecido, al menos, una notificación a la Comisión sobre el proceso de transposición en marcha.

En cuanto a las conclusiones del informe sobre la implantación de la normativa comunitaria en sus ordenamientos penales, constata que la Decisión Marco está aún en fase de transposición en algunos Estados miembros pero que se han registrado notables progresos en los veinte Estados evaluados en el informe, estimando que el grado de aplicación de la normativa comunitaria es satisfactorio. Además, señala que su preocupación principal se centra en los siete Estados miembros que todavía no han comunicado ninguna medida de transposición.

Finalmente concluye con la llamada a la revisión constante de las legislaciones en materia de delincuencia informática a fin de combatir de la forma más eficaz este tipo de delincuencia.

c.3. La propuesta de Directiva relativa a los ataques contra los sistemas de información.

Como ya hemos introducido en el apartado anterior, en la actualidad está en fase de aprobación una Directiva que derogue la actual Decisión Marco 2005/222/JAI. El texto consolidado de esta propuesta de Directiva es de fecha 30 de septiembre de 2010[294], si bien sobre este texto existen informes recomendando su revisión en algunos extremos, encontrándose, en todo caso, todavía en fase de negociación[295].

Lo primero en lo que debemos detener el análisis es el cambio de instrumento para la regulación de las conductas objeto de este estudio. Se pretende modificar el origen de la misma, pasando de la figura de la Decisión Marco a la de la Directiva. Sobre este asunto, debemos referirnos a la mejor elección de instrumento, por cuanto el método más correcto de regulación es a través de la Directiva, y no de la Decisión, como ha sido realizada la todavía vigente regulación. Esto es así porque, aun existiendo la figura de la Decisión normativa y su obligatoriedad (artículo 288 del Tratado de Funcionamiento de la Unión Europea) su configuración tiene como idea principal la de afectar a una serie de destinatarios seleccionados y no a un conjunto o totalidad de Estados como es el caso real en el que nos encontramos. Pero es que además, cuando esa Decisión no sólo afecta a un conjunto de destinatarios sino que también tiene por objetivo la adopción de medidas de carácter general por los Estados, su función normativa queda entonces solapada con la de la Directiva[296],

[294] COM(2010)517 final, de 30 de septiembre de 2010, de Propuesta de Directiva del Parlamento Europeo y del Consejo relativa a los ataques contra los sistemas de información, por la que se deroga la Decisión Marco 2005/222/JAI del Consejo.

[295] Para una visión exhaustiva, los documentos relativos a esta propuesta legislativa se agrupan en el Expediente interinstitucional 2010/0273 (COD) del Consejo de la Unión Europea.

[296] ALONSO GARCÍA, R.: *Sistema Jurídico de la Unión Europea*, Ed. Thomson Reuters, 2ª edición, Navarra, 2010, p. 131.

siendo por tanto la elección de ésta segunda la más acertada[297]. Mientras que la Decisión Marco tenía su origen legislativo esencialmente en el Consejo, en el cual el Parlamento Europeo tuvo una actuación relativamente menor[298], la propuesta de Directiva tiene su origen normativo el Parlamento Europeo e igualmente en el Consejo a través del sistema de codecisión[299] de tal forma que se pretende una mayor participación del Parlamento, no sólo en la toma de decisión sino también en la elaboración de la misma.

Analizando el contenido de dicha propuesta de Directiva en relación con el contenido de la Decisión Marco vigente, resulta esclarecedora su exposición de motivos, en la que viene a enumerar las cuestiones que han resultado de especial preocupación en el seno de las instituciones europeas y que han provocado la necesidad de otorgar a los Estados miembros de una actualización de las conductas peligrosas que ya quedaron anunciadas en la anterior Decisión Marco 2005/222/JAI de 24 de febrero. La propia exposición de motivos establece que el objeto de la nueva Directiva es sustituir a la Decisión Marco vigente e incluir una serie de medidas para proteger los sistemas de información de ataques que no estaban en el centro de atención cuando fue promovida la anterior regulación. Se focaliza en un determinado nuevo sistema de acceso y daños a los sistemas de información (*botnets*[300]). Pero este es sólo uno de los ámbitos con los que se pretende completar

[297] Esta orientación parece ser la seguida por la Unión Europea como se desprende de la sustitución (y ampliación) de la Decisión Marco relativa a la pornografía infantil y otros delitos conexos de 2004, por una Directiva sobre la misma materia en 2011.

[298] El Artículo 192 del Tratado Constitutivo de la CE regula el procedimiento de consulta**,** consistiendo en que el Parlamento emita su dictamen sobre la propuesta de legislación antes de que el Consejo proceda a su adopción de conformidad con el artículo.

[299] El Artículo 294 del Tratado de Funcionamiento de la UE (antiguo artículo 251 del Tratado Constitutivo de la CE) regula el procedimiento de codecisión que constituye el procedimiento legislativo central del sistema de toma de decisiones comunitario actual. Este procedimiento se basa en la búsqueda de un acuerdo entre el Parlamento Europeo y el Consejo para que el proceso legislativo alcance un resultado.

[300] El Instituto Nacional de Tecnologías de la Comunicación, S.A. (INTECO), sociedad mercantil dependiente del Ministerio de Industria, Turismo y Comercio, establece que *botnets* o redes *zombie* son conjuntos de ordenadores que han sido infectados con un tipo de *software* malicioso que permite al atacante controlar dichas máquinas sin tener acceso físico a ellas y sin el conocimiento del propietario. Ya ha sido objeto de estudio en el capítulo primero.

la vigente normativa[301]. Así, se añadirá también la acción típica de interceptación ilícita a las tres acciones ya contempladas en el análisis de la Decisión Marco. Se prevé la penalización de la producción, la venta, la adquisición para el uso, la importación, la distribución y cualquier otra forma de puesta a disposición de los dispositivos utilizados para cometer las infracciones reguladas[302]; así como la inclusión de una serie de agravantes relacionadas con los ataques a gran escala, los medios utilizados en la comisión de las acciones típicas, así como una relativa a métodos de ocultación de la identidad del autor. En último término, se introducirán medidas para mejorar la cooperación judicial europea en materia penal mediante el reforzamiento de la estructura existente y se abordará la necesidad de proporcionar datos estadísticos sobre la ciberdelincuencia, imponiendo a los Estados miembros la obligación de garantizar el establecimiento de un sistema adecuado de recogida, producción y suministro de datos estadísticos sobre las infracciones penales a que se refiere la Decisión Marco existente, así como de la interceptación ilícita que será incluida en la regulación.

Más allá de estas incorporaciones cabe mencionar que, en cuanto al análisis de las conductas de daños informáticos que se abordarán en la segunda parte de la investigación, no parece que la presumible aprobación de esta nueva Directiva vaya a modificar nada de lo ya referido cuando nos detuvimos en la regulación de los daños que establece la vigente Decisión Marco de 2005, aunque sí se complementará con la tipificación del abuso de dispositivos que aparece por primera vez como conducta penalmente típica en el ámbito de las conductas reguladas, así como, quizá, la aparición de nuevos supuestos agravados, lo que producirá una nueva necesidad de revisión de la legislación penal española, que no contempla dichos extremos en su ordenamiento.

Nos parece correcto, por último, aplaudir la decisión de obligar a los Estados a obtener estimaciones estadísticas propias sobre los niveles de ciberdelincuencia. Hecho que no se ha venido produciendo, por cuanto la mayor parte de las fuentes de

[301] Siguiendo las recomendaciones de la comunicación COM(2006)688 final, de 15 de noviembre de 2006, sobre lucha contra el *spam*, los programas espía y los programas maliciosos.

[302] Es decir, el abuso de dispositivos, que ya estaba tipificado en el Convenio sobre la Ciberdelincuencia de 2001 en su artículo 6, pero no así en la Decisión Marco de 2005.

datos sobre la existencia de delincuencia informática tenía como referencia los estudios hechos por compañías privadas de seguridad en la red. Los datos de los diferentes Estados, miembros o no de la Unión, -cuando existían- eran dispersos y basados en diferentes baremos. Lo que nos permite afirmar lo ilógico que resulta que un Estado, o la propia Unión Europea, dependa casi exclusivamente de los datos que estas fuentes externas les proporcionen para dirigir sus propuestas de política criminal.

D) LA LUCHA CONTRA LA CIBERDELINCUENCIA EN LA UNIÓN EUROPA EN LA ACTUALIDAD

A diferencia de lo ocurrido a principios de este siglo XXI, en el que los instrumentos de la Unión Europea en materia de lucha contra la delincuencia informática han sido escasos (pero importantes), en el último lustro la consideración que en el seno de la institución ha tomado esta materia se ha multiplicado exponencialmente, hasta el punto de existir varias comunicaciones al respecto que abordan diversos extremos, labores activas en materia de prevención y persecución del delito, así como la propuesta de Directiva ya analizada. Por ello, aunque el carácter imperativo de los siguientes instrumentos es menor, suponen, con diferencia, el camino más adecuado para una correcta lucha contra este tipo de delincuencia en el seno de la Unión Europea en la actualidad y para el futuro más próximo.

d.1. Comunicación acerca de dirigirse hacia una política general de lucha contra la ciberdelincuencia de 2007.

Esta comunicación de la Comisión al Parlamento Europeo, al Consejo y al Comité de las Regiones[303], posterior a la aprobación de las Decisiones Marco relativas a la pornografía infantil y los delitos informáticos, tiene por objeto fijar una política general destinada a mejorar la coordinación de la lucha contra la delincuencia informática a escala europea e internacional. En dicha comunicación, además de realizarse un repaso a los instrumentos internacionales existentes en ese momento, se enuncian medidas para hacer frente a este fenómeno y mejorar la colaboración entre los distintos protagonistas en la Unión Europea, relacionadas con

[303] COM(2007)267 final, de 22 de mayo de 2007.

incrementar la cooperación operativa de las autoridades policiales y judiciales, aumentar la cooperación y la coordinación políticas entre los Estados miembros y la cooperación política y jurídica con terceros países, así como fomentar las relaciones de diálogo con la industria del sector, la sensibilización, la formación y la investigación en este ámbito[304].

La Comisión propone a tal efecto: establecer una cooperación operativa reforzada entre las autoridades policiales y judiciales de los Estados miembros, aumentar el presupuesto financiero concedido a las iniciativas destinadas a mejorar la formación de las autoridades policiales y judiciales en materia de delincuencia informática, ayudar a la investigación en este ámbito, iniciar acciones que asocien a los sectores público y privado y se centren en la sensibilización de la población, en especial los consumidores, sobre los costes y peligros que entraña la ciberdelincuencia, fomentar la cooperación internacional global en materia de lucha contra la ciberdelincuencia o adoptar medidas concretas para animar a todos los Estados miembros y terceros países pertinentes a ratificar el Convenio del Consejo de Europa sobre la Ciberdelincuencia; entre otras medidas en esta línea de colaboración y sensibilización. Además se recuerda, dentro del ámbito legislativo de la Unión Europea, la importancia de la lucha contra la delincuencia tradicional que utiliza las redes informáticas para favorecer la comisión de los delitos y propone la elaboración de trabajos en el ámbito normativo específico de la Unión Europea contra la usurpación de identidad, el fraude, el comercio ilícito o la lucha contra contenidos ilícitos en Internet[305].

[304] "Nueva estrategia comunitaria contra el cibercrimen: La Comisión europea presenta una comunicación" en *Europa Euskadi*, nº 220, 2007, p. 24.

[305] La propuesta de la Comisión relativa a los contenidos ilícitos es la más novedosa en algunos aspectos. Tiene por objetivo seguir elaborando medidas de lucha contra contenidos ilícitos específicos, en especial los que se refieren al abuso sexual de menores, pero también relativos a la apología del terrorismo, instar a los Estados miembros a asignar recursos financieros suficientes para intensificar la labor de los servicios policiales y judiciales, en especial las medidas de identificación de las víctimas de abusos sexuales que puedan aparecer en material gráfico distribuido en línea, apoyar medidas de lucha contra los contenidos ilícitos que puedan incitar a los menores a adoptar comportamientos violentos, promover el diálogo entre los Estados miembros y con terceros países sobre las técnicas de lucha contra los contenidos ilícitos y sobre los procedimientos de cierre de sitios web ilegales y elaborar acuerdos en la UE, entre las autoridades públicas y los operadores privados, especialmente

Se señala la insuficiencia de estadísticas respecto de la delincuencia informática. Cabe destacar que si en la exposición de motivos de la Decisión Marco 2005/222/JAI de 24 de febrero del Consejo se encuentran referencias veladas a datos reales y objetivos que han llevado al legislador a decidirse por el camino tomado[306], es lógico pensar que para obtener una idea del problema común que supone la ciberdelincuencia, debemos referirnos a las estadísticas que se manejan sobre la misma. Dos son las fuentes principales que ha utilizado la Unión Europea en los años precedentes; por un lado, las fuentes gubernamentales basadas en las estadísticas policiales o judiciales y, por otro, las fuentes privadas, esto es, estudios que realizan las principales empresas del sector comunicaciones y de seguridad informática. Empezando por el análisis de las fuentes gubernamentales, a diferencia de lo observado al referirnos a las diferentes agencias norteamericanas encargadas de la seguridad en la red, que realizan anualmente seguimientos estadísticos de afectación por la ciberdelincuencia, repercusión económica, nivel de tolerancia, etc.[307], en Europa no existían estadísticas comunes en materia de ciberdelincuencia, es decir, realizadas por instituciones europeas. Es más, hasta el informe del año 2009 de la *Europol*[308] que bajo la rúbrica *High-Tech Crime* analiza la situación actual en Europa en relación con estos delitos, no se había incluido referencia alguna a este tipo de delincuencia en las memorias anuales que realiza el citado organismo. Precisamente a ello hace referencia en el propio informe de 2009 en el que analiza que "la lucha contra la ciberdelincuencia pasa a ser una prioridad de la agenda europea, y por tanto también de la *Europol*".

---

los proveedores de servicios de internet, relativos a los procedimientos de bloqueo y cierre de los sitios ilegales en Internet.

[306] La consideración 2ª de la Decisión Marco 2005/222/JAI, de 24 de febrero del Consejo, cuando se refiere a que "se ha comprobado la existencia de ataques contra los sistemas de información, en particular como consecuencia de la amenaza de la delincuencia organizada, y crece la inquietud ante la posibilidad de ataques terroristas contra sistemas de información que forman parte de las infraestructuras vitales de los Estados miembros", parece estar basando su afirmación en estadísticas policiales y/o judiciales de los diferentes países miembros.

[307] Se puede acceder gratuitamente a las estadísticas desde las diferentes webs norteamericanas de las instituciones mencionadas en este estudio.

[308] Organismo creado a partir del Tratado de la Unión Europea cuya misión es la de facilitar las operaciones de lucha contra la criminalidad en el seno de la Unión Europea, con competencia en los 27 Estados miembros.

Por tanto, las fuentes gubernamentales a las que se puede acudir para valorar el efecto real de la delincuencia informática en Europa pasaban por el análisis separado de las estadísticas judiciales o policiales de cada uno de los Estados miembros, lo que lógicamente complica la idea de dar una visión general europea del problema en el momento en que se aprueban las decisiones marco de 2003 y 2005[309].

Sin embargo, otro tipo de fuentes que se han demostrado fiables para el análisis de la delincuencia informática son las que nos proporcionan las empresas privadas, normalmente aquellas dedicadas a la seguridad en la red. Así, es habitual encontrar informes anuales de las principales compañías de seguridad[310] en los que sí se puede observar como el crecimiento de los delitos informáticos ha sufrido un aumento durante la primera década del siglo XXI.

Hemos de suponer, por tanto, que cuando el legislador europeo hacía referencia en el considerando segundo de la Decisión Marco al hecho de que se ha venido observando la existencia de ataques a sistemas de información, dicha reflexión es fruto del análisis de estas fuentes de estadísticas: por un lado, las de origen gubernamental de los Estados miembros y, por otro, las de las empresas de seguridad informática; e igualmente de los informes que las diferentes agencias estadounidenses manejan sobre este asunto. Quizá la crítica que cabe realizar en este aspecto, es la falta de una estadística europea común, de origen gubernamental, que pueda facilitar una visión general de la situación real que existe en el viejo continente. No se trata de poner en duda la fiabilidad de los informes realizados por iniciativas privadas o por los Estados miembros, pero parece lógico pensar que el gigante aparato administrativo que es la Unión Europa debería trabajar con sus propias estadísticas y no con las de terceros; ya sean estos los propios Estados miembros, Estados no miembros, o empresas privadas.

Lo cierto es que esta situación parece haberse corregido en la medida en que

[309] Se ha señalado en la introducción de la investigación como en el caso español no existen estadísticas fiables al respecto y no ha sido hasta el año 2012 cuando se ha implantado un sistema de estadísticas a través de las actuaciones del Ministerio Fiscal, siendo hasta este momento las fuentes de datos más fiables las denuncias presentadas ante las Fuerzas y Cuerpos de Seguridad del Estado.

[310] Por citar algunas de las más conocidas: Mcafee, Norton, Panda, Eset o Kaspersky Lab.

en 2008, bajo la Presidencia francesa de la Unión Europea, se impulsó la creación de una Plataforma Europa de Cibercrimen (ECCP[311]), órgano dependiente de la Europol, cuya misión será reportar todos los actos sospechosos relacionados con la ciberdelincuencia, así como coordinar la estrategia común para la lucha contra estos delitos informáticos, labores que nos recuerdan al ya comentado *Internet Crime Complaint Center* (IC3) puesto en marcha en Estados Unidos en el año 2000[312]. Lo cierto es que dicho organismo de la Unión Europea no ha comenzado su actividad hasta Enero de 2013, bajo el nombre de Centro Europeo de Ciberdelincuencia (EC3[313]), lo que no nos permite, por ahora, añadir nada más a lo ya indicado.

d.2. Comunicación acerca de proteger Europa de ciberataques e interrupciones a gran escala de 2009.

En 2009 se emite la Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones sobre protección de infraestructuras críticas de información titulada "Proteger Europa de ciberataques e interrupciones a gran escala: aumentar la preparación, seguridad y resistencia", de fecha 30 de marzo de 2009[314]. Dicho interés, como señala la comunicación, parte de las estimaciones del Foro Económico Mundial del año 2008 en el que se calculó que las probabilidades de que las infraestructuras críticas relativas a los sistemas informáticos sufrieran un fallo importante en los siguientes diez años oscilaban entre el 10 y el 20 %, cuyo coste podrían suponer entre 250.000 millones y un billón de dólares debido a que un ataque contra estos sistemas de información crearía un efecto dominó que podría afectar a otras infraestructuras como el agua, la energía o el transporte[315]. Como muestra de la gravedad de la situación ejemplifica los ciberataques lanzados en Estonia, Lituania o Georgia que confirmaban la necesidad de líneas de acción coordinadas.

---

[311] Siglas en inglés de *European Cyber Crime Platform.*

[312] Entre 2000 y 2003 bajo el nombre de *Internet Fraud Complaint Center* (o IFCC) y ya a partir de 2003 con la actual nomenclatura de *Internet Crime Complaint Center* (o IC3).

[313] Siglas en inglés de *European Cybercrime Centre*, plenamente operativa a partir del 9 de enero de 2013.

[314] COM(2009)149 final, de 30 de marzo de 2009.

[315] WEF: *Global Risk 2008,* Ed. World Economic Forum, 1ª edición, Ginebra, 2008, pp. 22 y 23.

En la Comunicación, de nuevo, se resuelve que las actividades cotidianas, privadas y profesionales dependen cada vez en mayor medida del desarrollo de los sistemas informáticos y las tecnologías de la información y de la comunicación, y como consecuencia de ello, la protección de las infraestructuras críticas de información[316] frente a la delincuencia informática a gran escala representa un importante reto para la sociedad y la economía europeas. Igualmente, se enumeran los principales desafíos a los que se enfrentan estas infraestructuras críticas de información (virus informáticos, gusanos, *botnets* y en general *software* malicioso, así como correo no deseado con fines maliciosos) y propone un plan de acción dirigido a reforzar su protección.

Se señala que aunque la elaboración de las políticas relacionadas con las infraestructuras críticas de información compete en última instancia a los Estados miembros, su aplicación depende de la intervención del sector privado, que posee o controla un buen número de ellas, lo que hace necesaria la colaboración público-privada para una protección eficaz.

Por ello, respecto de los puntos expuestos, la Comisión propone un plan de acción articulado en torno a cinco ejes:

1.- Preparación y prevención: se insta a los Estados miembros a definir, con la ayuda de la Agencia Europea de Seguridad de las Redes y de la Información (ENISA[317]), un nivel mínimo de capacidades y servicios para los Equipos de

[316] Según la comunicación COM(2005)576 final, se entiende por infraestructuras críticas de la Unión Europea (entre las que se incluyen las relativas a los sistemas de información) "los recursos físicos, servicios y sistemas de tecnologías de la información, redes y elementos de infraestructura cuya interrupción o destrucción tuviera grave impacto en la salud, la seguridad o el bienestar económico o social".

[317] Siglas en ingles de *European Network and Information Security Agency*, creada por el Reglamento (CE) n º 460/2004 del Parlamento Europeo y del Consejo, de 10 de marzo de 2004, la misión de la Agencia es esencial para lograr un nivel elevado y efectivo de seguridad de las redes de la información dentro de la Unión Europea. Junto con las instituciones de la UE y los Estados miembros, la ENISA pretende desarrollar una cultura de seguridad de las redes de la información para el beneficio de los ciudadanos, los consumidores, las empresas y las organizaciones del sector público en la Unión Europea. Además, su función consiste en ayudar a la Comisión Europea, los Estados miembros y la comunidad empresarial para abordar, responder y sobre todo para evitar problemas de red y seguridad de la información. La ENISA está formada por un cuerpo de expertos creado por la UE destinado a llevar a cabo tareas técnicas específicas en el campo de la Seguridad de la Información

Respuesta ante Emergencias de Informáticas (CERT[318]) nacionales. Además, la Comisión pondrá en marcha una asociación público-privada europea de resistencia sobre objetivos y de mejora de la seguridad y la resistencia. También se establecerá un Foro europeo para facilitar el intercambio de información entre los Estados miembros.

2.- Detección y respuesta: se desarrollará y pondrá en marcha un Sistema Europeo de Intercambio de Información y Alerta (EISAS[319]), que llegue a los ciudadanos y las PYMEs.

3.- Mitigación y recuperación: se insta a los Estados miembros a elaborar planes nacionales de contingencia, a organizar ejercicios de simulación de incidentes a gran escala de seguridad de las redes y a estrechar la cooperación entre los equipos CERT nacionales. La Comisión apoya financieramente la realización de ejercicios paneuropeos que también podrán constituir la plataforma operativa para la participación paneuropea en ejercicios internacionales.

4.- Cooperación internacional: se prevé la cooperación internacional en lo que respecta principalmente a la resistencia y estabilidad de Internet para la definición de prioridades, principios y directrices. En primer lugar a escala europea y después a nivel mundial.

5.- Y por último se insta al establecimiento de criterios relativos a infraestructuras críticas europeas en el ámbito de los sistemas informáticos, que partiendo de la definición común, y sin contradecirla, especifiquen en éste ámbito cuales son las peculiaridades y los aspectos singulares a tener en consideración en las políticas de la Unión y de los Estados miembros.

---

así como asistir a la Comisión Europea en los trabajos técnicos preparatorios para la actualización y desarrollo de la legislación comunitaria en el ámbito de la seguridad de las redes y de la información: http://www.enisa.europa.eu/

[318] Siglas en inglés de *Computer Emergency Response Team*.

[319] Siglas en inglés de *European Information Sharing and Alert System*. Para una visión específica del sistema y su funcionamiento ver EISAS: *European Information Sharing and Alert System. A Feasibility Study 2006/2007*:
http://www.enisa.europa.eu/activities/cert/other-work/eisas_folder/EISAS_finalreport.pdf

La comunicación concluye recordando que "la mejora de la seguridad y resistencia de las infraestructuras críticas de información es un objetivo a largo plazo, cuya estrategia y medidas requieren evaluaciones periódicas", por lo que la revisión de estas políticas deberá realizarse periódicamente en el futuro.

d.3. Comunicación sobre la protección de infraestructuras críticas de información de 2011.

En consonancia con la importante política europea iniciada por la comunicación de 2009, en el año 2011 se emite la Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones relativa a la protección de infraestructuras críticas de información sobre "logros y las próximas etapas: hacia la ciberseguridad global"[320].

En ella, se recuerda en primera instancia la Comunicación de 30 de marzo de 2009 (*supra*), por la que se implantaba un plan de acción de protección de infraestructuras críticas de la información cuyo objetivo era fortalecer la seguridad y la resistencia de las infraestructuras vitales de las tecnologías de la información y comunicación sustentado en los cinco pilares ya expuestos; así como otros puntos señalados en la Agenda Digital para Europa[321] tales como iniciativas sobre seguridad en las tecnologías de la información que permitan la actuación inmediata de los organismos nacionales y europeos, así como medidas en el ámbito penal y jurisdiccional para agilizar dicha protección[322]. También se recuerda brevemente los peligros a los que está expuesta la sociedad en la actual cultura de la información y comunicación[323] y añade que tales peligros "no son privativos de la Unión Europea,

[320] COM(2011)163 final, de 31 de marzo de 2011.

[321] COM(2010)245 final/2, de 26 de agosto de 2010, acciones 6 y 7 relativas al punto 2.3 "confianza y seguridad".

[322] Entre las que se encuentra la Propuesta de Directiva relativa a los ataques contra los sistemas de información o un fortalecimiento de la Agencia Europea de Seguridad de las Redes y de la Información (ENISA) con el objeto de impulsar la confianza en la red, así como su seguridad.

[323] Realiza una nueva clasificación de las amenazas que surgen en el marco de la delincuencia informática según los fines que persiguen: a) fines de explotación, como es el caso de las amenazas de espionaje económico y político, los robos de identidad, o los recientes ataques contra el sistema de comercio de derechos de emisión o contra los sistemas de los Estados; b) fines de perturbación, como la denegación de servicio distribuido o el *spam* generado vía *botnets*, o el corte de los medios de comunicación, y c) fines de destrucción física; esta es una posibilidad que todavía no se ha presentado pero, vista la omnipresencia creciente de las TIC en las infraestructuras críticas no cabe descartarla en

ni pueden ser resueltos por ella aisladamente. La omnipresencia de las TICs y de Internet permite que la comunicación, la coordinación y la cooperación entre los diferentes actores sea más eficaz, eficiente y económica, y da como resultado un dinámico ecosistema de innovación en todos los ámbitos de la vida. Pero el peligro puede surgir de cualquier lugar del mundo y, debido a la interconexión global, repercutir en cualquier lugar del mundo".

Para combatir de la mejor forma estos peligros, y siguiendo la línea de la comunicación de 2009, la presente revisa según la estructura de aquella los resultados logrados desde la adopción del plan de acción en 2009, a la vez que expone las próximas etapas que se han programado para cada acción tanto a nivel europeo como internacional:

1.- Preparación y prevención: en 2009 la ENISA, en colaboración con la comunidad de CERTs de Europa desarrollaron y aprobaron un conjunto mínimo de capacidades y servicios de referencia que deben poseer los CERTs nacionales -en los ámbitos del funcionamiento, la capacidad técnica, los mandatos y la cooperación- para poder funcionar de forma efectiva en pro de la cooperación europea. En 2010 la ENISA trabajó con la comunidad de CERTs de Europa para convertir los requisitos anteriores, fundamentalmente orientados al funcionamiento, en una serie de recomendaciones de política destinadas a los CERTs nacionales para que pasen a ser el factor principal de la preparación, la difusión de información, la coordinación y la respuesta. Hasta la fecha, veinte Estados miembros han desarrollado CERT nacionales[324] y casi todos los demás tienen previsto hacerlo. Como se anunció en la

---

los próximos años (provocar inundaciones alterando los sistemas informáticos que regulan los recursos hidrográficos, catástrofes derivadas de la manipulación informática de sistemas que gestionan el correcto funcionamiento de las centrales eléctricas, etc.).

[324] En España el Instituto Nacional de Tecnología de la Comunicación (INTECO), organismo dependiente del Ministerio de Industria, Energía y Turismo de España (http://cert.inteco.es) y el Centro Nacional de Inteligencia (CNI), organismo dependiente del Ministerio de Presidencia (https://www.ccn-cert.cni.es/) realizan ambos las labores de CERT nacional, mientras que el primero tiene como público a los ciudadanos y empresas, el segundo está orientado a las administraciones públicas. INTECO-CERT (@IntecoCert). "@jalexandre85 Efectivamente, cada uno tenemos un público objetivo diferente y son los que has mencionado. Un saludo!" 5 nov 12, 6:07 p.m. Tweet. Los menciona ALAMILLO DOMINGO, I.: "Las políticas… ob. cit. pp. 13 y 14. Además, en enero de 2013 se ha puesto en funcionamiento un nuevo CERT bajo el mando de la Policía Nacional (dependiente del Ministerio de Interior), lo que parece un claro caso de duplicidad (triplicidad) de organismos con una función esencialmente igual, cuestión que es ajena a nuestro estudio, pero que cabe al menos señalar.

Agenda Digital para Europa, la Comisión ha propuesto medidas para establecer un CERT al servicio de las instituciones europeas para 2012[325]. En 2009 se puso en funcionamiento la Asociación Europea Público-Privada para la resiliencia[326] (EP3R[327]) cuyo objetivo es constituir un marco de gobernanza europea para la resistencia de las infraestructuras de tecnologías de la información, que trate de fomentar la cooperación entre el sector público y el privado en torno a objetivos de seguridad[328]. Igualmente en el año 2009 se instituyó el Foro Europeo para Estados Miembros (EFMS[329]) con el fin de fomentar el debate y el intercambio entre las autoridades públicas en materia de buenas prácticas y de compartir objetivos y prioridades políticas en materia de seguridad y resistencia de las infraestructuras informáticas y de telecomunicaciones

Como objetivos para los próximos años se establece continuar la labor de instaurar CERT nacionales en los Estados restantes hasta completarse en todos los miembros de la Unión Europea, para una vez conseguido, analizar la conveniencia de

[325] El CERT-Europa se encuentra en funcionamiento desde el 11 de septiembre de 2012 y se define como un equipo formado por expertos en seguridad informática de las principales instituciones de la UE (Comisión Europea, la Secretaría General del Consejo, Parlamento Europeo, Comité de las Regiones y Comité Económico y Social) que coopera estrechamente con otros CERT en los Estados miembros y no miembros, así como con empresas especializadas en seguridad informática: http://cert.europa.eu

[326] Aunque la RAE no contiene una acepción adecuada en esta materia, la resiliencia en términos de informática y telecomunicaciones es la capacidad de un sistema (informático, se entiende) de soportar y recuperarse de desastres o perturbaciones.

[327] Siglas en inglés de *European Public-Private Partnership for Resilience*. Sus objetivos, principios y estructura se describen en el documento sobre el establecimiento de la EP3R elaborado en junio de 2010:
http://ec.europa.eu/information_society/policy/nis/docs/ep3r_workshops/3rd_june2010/2010_06_23_ep3r_nonpaper_v_2_0_final.pdf

[328] Bajo el auspicio de la EP3R, antes de terminar el año 2010 se pusieron en funcionamiento tres grupos de trabajo sobre los siguientes puntos: a) los bienes, recursos y funciones imprescindibles para la provisión continuada y segura de comunicaciones electrónicas en todos los países; b) los requisitos de referencia para la seguridad y resistencia de las comunicaciones electrónicas y c) las necesidades de coordinación y cooperación y los mecanismos necesarios para prevenir y reaccionar ante perturbaciones a gran escala que afecten a las comunicaciones electrónicas.

[329] Siglas en inglés de *European Forum for Member States.* Este foro se reúne de forma trimestral desde el año 2010 y ha efectuado progresos significativos en diferentes campos: a) la fijación de criterios que identifiquen las infraestructuras europeas de las TICs en el contexto de la Directiva sobre la identificación y designación de infraestructuras críticas europeas; b) la determinación de prioridades, principios y directrices europeas para la resistencia y estabilidad de Internet y c) el intercambio de buenas prácticas, en particular en materia de ciberejercicios.

ampliar sus capacidades y convertirlos en "la espina dorsal" del Sistema Europeo de Intercambio de Información y Alerta (EISAS) al servicio de los ciudadanos y las PYMEs. Se debe seguir fomentando la labor de la Asociación Europea Público-Privada para la resiliencia (EP3R) con el fin de adaptar la seguridad y la resistencia respecto de nuevos ataques basados en instrumentos innovadores. Utilizando como base la labor preparatoria efectuada por la Comisión y la ENISA, los futuros trabajos abordarán los problemas de ciberseguridad que se plantean para las redes inteligentes, así como respaldar las actividades del Grupo de trabajo UE-EEUU sobre ciberseguridad y ciberdelincuencia al objeto de crear un entorno coherente de cooperación entre los sectores público y privado. Igualmente se prioriza la orientación tanto de la ENISA, como el EFMS hacia labores generales relacionadas con: a) la cooperación efectiva entre los CERT nacionales, b) la promoción de requisitos mínimos en el ámbito de la contratación pública con el fin de fomentar la ciberseguridad y c) la evaluación del estado de salud de la ciberseguridad en Europa.

2.- Detección y respuesta: La ENISA realizó una elaborada hoja de ruta para la creación del Sistema Europeo de Intercambio de Información y Alerta (EISAS)[330].

Las siguientes etapas previstas se basan en el apoyo a los Estados miembros en la ejecución de la hoja de ruta del EISAS, cuyo objetivo principalmente se encuentra en desarrollar los servicios básicos que utilizarán los Estados miembros para crear su Sistema de Intercambio de Información y alerta a partir de sus CERT nacionales para que la ENISA pueda desarrollar servicios de interoperabilidad que permitan a cada Sistema de Intercambio de Información nacional integrarse en ella.

3.- Mitigación y recuperación: Se han comenzado a desarrollar planes nacionales de contingencia y organizado ejercicios de respuesta ante incidentes a gran escala de seguridad de las redes y de recuperación en caso de catástrofes antes de finalizar el año 2010. Además la ENISA ha elaborado una guía de buenas prácticas para ejercicios nacionales y organizó en todo el mundo eventos con los Estados miembros a través de los CERT nacionales[331]. Por último cabe destacar el

[330] La hoja de ruta se puede consultar en la web de la ENISA: http://www.enisa.europa.eu/activities/cert/other-work/eisas_folder/eisas_roadmap.

[331] La ENISA ha difundido recomendaciones en materia de política de desarrollo de estrategias nacionales, en las que los CERT nacionales desempeñan un papel esencial a la hora de dirigir

fortalecimiento de la cooperación entre los CERT nacionales de los diferentes Estados de la Unión Europea.

Se proyecta para el futuro que la ENISA siga prestado su apoyo a los Estados miembros en la elaboración de los planes nacionales de contingencia y la organización de ejercicios periódicos de respuesta ante incidentes a gran escala de seguridad de las redes y de recuperación en caso de catástrofe, como vía hacia una cooperación paneuropea más estrecha. Además, se proyecta la realización de simulacros nacionales de ataques masivos a los sistemas informáticos y de telecomunicaciones de los Estados miembros de diversas magnitudes[332]. La ENISA trabajará con los Estados miembros en el desarrollo de un plan de contingencia en materia de ciberincidentes.

4.- Cooperación internacional: de los trabajos realizados por el Foro Europeo para Estados Miembros (EFMS), se han desarrollado unos principios y directrices europeos sobre resistencia y estabilidad de Internet[333]. Siete Estados miembros participaron en el ciberejercicio norteamericano "Cyber Storm III"[334] como asociados internacionales[335]. La Comisión y ENISA participaron como observadores.

En adelante se proyecta el debate y la promoción de estos principios tanto de forma bilateral con los socios internacionales, en particular los EE.UU., como de forma multilateral con el G8, la OCDE, Meridian y la UIT. La idea es que a partir de 2012 estos principios y orientaciones deberán constituir marco común de

---

ejercicios y ensayos nacionales de contingencia con la participación de agentes privados y públicos. El primer ejercicio paneuropeo sobre incidentes a gran escala de seguridad de las redes (Cyber Europe 2010) se celebró el 4 de noviembre de 2010 y contó con la participación de todos los Estados miembros.

[332] Los ciberejercicios constituyen un elemento importante de cualquier estrategia coherente de planificación de contingencias en materia de ciberincidentes, tanto a nivel nacional como europeo. Por lo tanto, los ciberejercicios paneuropeos futuros deben basarse en un plan europeo de contingencia en materia de ciberincidentes elaborado a partir de los planes nacionales de contingencia (que a la vez servirá para interconectarlos).

[333] La versión más actualizada, de marzo de 2011, se puede consultar en: http://ec.europa.eu/danmark/documents/alle_emner/videnskabelig/110401_rapport_cyberangreb_en.pdf

[334] En la actualidad se ha celebrado también el evento Cyber Storm IV. Los resultados de ambos se pueden consultar en la web dedicada del Departamento de Seguridad Nacional de los Estados Unidos. http://www.dhs.gov/cyber-storm-securing-cyber-space

[335] Francia, Alemania, Hungría, Italia, Holanda, Suecia y Reino Unido.

compromiso colectivo internacional en torno a la resistencia y estabilidad de Internet a largo plazo. Además, se debe continuar con la celebración de ciberejercicios de seguridad informática y de las telecomunicaciones de ámbito internacional, entre los Estados Unidos, la Unión Europea y, según las posibilidades, otras regiones o países que conozcan problemas similares con los que compartir estrategias y actividades.

5.- Por último, en relación al establecimiento de criterios relativos a infraestructuras críticas europeas en el ámbito de los sistemas informáticos, los debates técnicos en el Foro Europeo para Estados Miembros (EFMS) en torno a los criterios sectoriales específicos de las tecnologías de la información y comunicación han llevado al planteamiento -en fase inicial- de un proyecto de criterios aplicables a las comunicaciones móviles y fijas y a Internet. De forma paralela está prevista la celebración de consultas con el sector privado acerca del proyecto de criterios para el sector de las TICs.

La comunicación concluye, acertadamente, afirmando que "la experiencia demuestra que, a la hora de abordar cuestiones de seguridad y resistencia, un enfoque puramente nacional o regional no basta", y se recuerda que "Europa debe continuar sus esfuerzos para construir una estrategia coherente y cooperativa de toda la UE" en cuanto a la protección de los sistemas informáticos y de comunicación a largo plazo, para lo cual será esencial el papel de una Agencia Europea de Seguridad de las Redes y de la Información modernizada como pilar en el que puedan sustentarse los Estados miembros, las instituciones propias de la Unión Europea y también el sector privado.

Después de lo analizado podemos concluir estas líneas afirmando el ambicioso proyecto que ha emprendido la Unión Europea en cuanto la seguridad informática, no ya desde el ámbito exclusivo de la delincuencia informática, sino desde una perspectiva global (legislación, infraestructuras, organismos, etc.). No hablamos, por tanto, sólo de medidas legislativas puntuales, sino de una verdadera política de seguridad informática y de las telecomunicaciones acorde a las necesidades y características de la sociedad de la información actual. Entre otros aspectos, las instituciones europeas son conscientes de las graves consecuencias

sociales que pueden tener ataques informáticos con una motivación terrorista. La ciberdelincuencia es en realidad el paso previo al ciberterrorismo[336].

d.4. Comunicación sobre la represión del delito en la era digital y la creación de un centro europeo de ciberdelincuencia de 2012.

Siguiendo con las líneas marcadas por la comunicación de 2011, en el año 2012 se emite la Comunicación de la Comisión al Consejo y al Parlamento Europeo sobre la represión del delito en la era digital: creación de un centro europeo de ciberdelincuencia[337]. En ella, una vez más recordando que los sistemas informáticos e Internet (que describe como espacio abierto, sin límites nacionales ni una estructura de gobernanza) se han convertido en una parte indispensable de nuestra sociedad en todos los aspectos, se hace mención al multimillonario coste que supone para la sociedad actual la delincuencia informática[338]. Dicha comunicación se centra, concretamente, a diferencia de las anteriores que lo hacían desde una perspectiva general, en el ámbito de la delincuencia informática

Por ello, ante esta situación, la Unión Europea ha desarrollado iniciativas concretas en el ámbito penal para contrarrestar los efectos que produce la diversidad legislativa de los Estados miembros en este ámbito. Así se aprobaron en los años 2003 y 2005 dos Decisiones Marco relativa la primera al abuso de menores y la pornografía infantil en la que aparecían los sistemas informáticos y las redes, y la segunda centrada en otro tipo de delincuencia informática relacionada con el fraude

[336] CHICHARRO LÁZARO, A.: "La labor…" ob. cit. pp. 3 y 4, señala que "así, *ciberterrorismo* será la forma de terrorismo que emplea las tecnologías de la información y la comunicación para someter a los poderes públicos, a ciertos individuos o grupos de la sociedad, o, de manera general, a la opinión pública, a un clima de terror, con el fin de lograr sus aspiraciones.[…] El ciberterrorismo es una conducta ilícita de los denominados *cibercrímenes* o *delitos informáticos*, en los que un elemento esencial es la utilización de ordenadores como instrumentos o como objetivos produciendo un clima de terror, para que se dé el tipo penal". A este respecto también se refiere MAGRO SERVET, V.: "La delincuencia informática. ¿Quién Gobierna Internet?" en *Diario La Ley*, nº 6077, 2004 y SÁNCHEZ MEDERO, G.: "Internet: Un espacio para el cibercrimen y el ciberterrorismo" en *Crisis analógica, futuro digital: actas del IV Congreso Online del Observatorio para la Cibersociedad, celebrado del 12 al 29 de noviembre de 2009*, Ed. Meddia, cultura i comunicació, edición electrónica, 2010: http://www.cibersociedad.net/congres2009/actes/html/com_internet-un-espacio-para-el-cibercrimen-y-el-ciberterrorismo_610.html

[337] COM(2012)140 final, de 28 de marzo de 2012.

[338] Norton Cybercrime Report 2011, Symantec, 7 de septiembre de 2011, consultado el 6 de enero de 2012.

informático, la falsificación electrónica, la intromisión ilícita o los daños informáticos. En la actualidad, además, la Decisión Marco de 2003 ha sido sustituida por una Directiva del año 2011 contra los abusos sexuales de los menores en línea y la pornografía infantil que mejora y amplía la regulación anterior y existe un proyecto de Directiva relativa a los ataques contra los sistemas de información, que igualmente amplía y corrige las deficiencias de la todavía vigente Decisión Marco de 2005 en ese ámbito, cuya aprobación se preveía para el año 2012[339]. Junto a estas herramientas de carácter legislativo se recuerda el también esencial papel que la Europol viene desempeñando y que deberá realizar en el futuro en relación con este tipo de delincuencia. En el marco de la cooperación internacional no olvida la importancia del Convenio sobre la Ciberdelincuencia de 2001 y la necesidad de conseguir que más Estados se adhieran al mismo, así como de estrechar las relaciones en la materia con los principales países de nuestro entorno al margen de la Unión Europea, especialmente con los Estados Unidos de América.

Bajo esta realidad, la comunicación establece una propuesta de constitución de un Centro Europeo de Ciberdelincuencia, (EC3) que dota de contenido a la originalmente planteada Plataforma Europa de Cibercrimen (ECCP) de 2008 y la acción prevista en la Agenda Digital Europea de 2010[340] en la que se proponen tres campos de actuación y cuatro funciones principales. Serán campos de actuación del EC3: a) los ciberdelitos cometidos por grupos de la delincuencia organizada, especialmente los que generan extensos réditos ilegales mediante el fraude en línea, b) los ciberdelitos que provocan daños graves a sus víctimas, como la explotación sexual de menores en línea y c) los ciberdelitos (incluidos los ciberataques) que afectan a infraestructuras y sistemas de información esenciales de la Unión Europea. Además sus funciones principales serán:

1.- Servir de punto central de información sobre la delincuencia en Europa: deberá reunir toda la información relacionada con la delincuencia informática en los Estados de la Unión Europea y del ámbito internacional a partir de todas las fuentes

[339] Que finalmente no se ha producido, si bien se espera que a lo largo del año 2013 sea definitivamente aprobada.

[340] COM(2010)245 final/2, de 26 de agosto de 2010, "otras acciones" relativas al punto 2.3 "confianza y seguridad".

disponibles en la actualidad -fuentes gubernamentales o de origen privado- que permitan completar los diferentes datos policiales disponibles[341].

2.- Aunar el conocimiento sobre ciberdelincuencia europea para contribuir a la capacitación de los Estados miembros: una de sus funciones principales es concentrar los conocimientos especializados en delincuencia informática para poder asistir a los Estados miembros y a sus funcionarios judiciales o policiales en labores de formación. Además, debe ser el eje sobre el que desarrollar manuales de buenas prácticas, así como punto de colaboración en el desarrollo de la cooperación internacional en la lucha contra la ciberdelincuencia.

3.- Prestar apoyo a los Estados miembros en investigaciones de ciberdelincuencia: fomentará la creación de equipos conjuntos de investigación e intercambio de información entre los Estados miembros para facilitar sus investigaciones nacionales.

4.- Ser la voz colectiva de los investigadores de ciberdelincuencia europeos ante los organismos de orden público y el estamento judicial: más que una función actual, se espera que con el tiempo el EC3 pueda también funcionar como punto de reunión de los investigadores europeos en el campo de la delincuencia informática además de convertirse en un foro de intercambio de profesionales de diversos ámbitos (judicial, policial, industrial, etc.).

El EC3, que ya es una realidad y se encuentra operativo desde el 11 de enero de 2013, se inscribe en la estructura de la Europol, pero sus labores no pueden suponer un ejercicio aislado dentro del organismo, de tal forma que deberán entablarse relaciones con otros actores interesados como Eurojust, la Escuela de Policía Europea (CEPOL[342]), los Estados miembros representados por el Grupo Especial de Ciberdelincuencia de la Unión Europea, la ENISA y la Comisión. La

[341] La comunicación señala como objetivo la posibilidad de dibujar un cuadro informativo de la delincuencia informática europea de tal forma que dichos datos permitan la elaboración de informes estratégicos sobre tendencias y amenazas y adquirir un adecuado conocimiento de la situación a partir de estadísticas delictivas amplias.

[342] Siglas en francés de *Collège Européen de Police.*

hoja de ruta marcada por la Comunicación establece como fecha límite para el funcionamiento completo del centro finales del año 2013[343].

5. TRASCENDENCIA EN NUESTRO ESTUDIO

Hemos visto como todos los conceptos y prácticas que señalamos en el capítulo primero, con el paso del tiempo, han sido conocidos por las instituciones nacionales e internacionales, que en mayor o menor medida han tratado de homogeneizar los ordenamientos jurídicos de sus Estados miembros marcando las directrices para penalizar estas conductas: ataques contra la integridad de la información contenida en sistemas informáticos, ataques contra páginas y servicios web, la creación de programas destinados a facilitar estas conductas, etc. En este capítulo segundo del presente estudio nos hemos detenido en el tratamiento que se ha dado a nivel internacional a la criminalidad informática tomando como referencia principal el Convenio sobre la Ciberdelincuencia del Consejo de Europa de Budapest, de 23 de noviembre de 2001 y la normativa de la Unión Europea, por ser instrumentos internacionales de obligado cumplimiento para nuestro país y, junto a ellos también hemos repasado otra suerte de recomendaciones e informes de diferentes organismos de relevancia internacional. Una vez expuesta la situación general en la que se encuentra el marco de la regulación en torno a la delincuencia informática, y antes de seguir profundizando nuestro estudio, baste por ahora señalar a modo de resumen, las más importantes clasificaciones que, sobre los delitos informáticos, se han realizado tanto a nivel internacional como a nivel estatal en España, clasificaciones que como veremos responden a muy diversas formas de interpretar el contenido del 'delito informático' como concepto.

[343] En la nueva web del organismo se puede leer que "tras un estudio de viabilidad realizado por Rand Corporation Europa, la Comisión Europea decidió crear un Centro Europeo Ciberdelincuencia (EC3) en Europol. El centro será el punto focal en la lucha de la UE contra la delincuencia informática, contribuyendo a reacciones más rápidas en caso de delitos en línea. Se apoyará a los Estados miembros y a las instituciones de la Unión Europea en el fomento de la capacidad operacional y analítico para la investigación y la cooperación con los socios internacionales": https://www.europol.europa.eu/ec3

A) CLASIFICACIÓN PRELIMINAR DE LOS DELITOS INFORMÁTICOS

En la actualidad es difícil hacer una clasificación clara de los delitos informáticos. Esto no se debe a que no estén, en mayor o menor medida, convenientemente regulados en nuestro ordenamiento penal, sino en que no existen criterios inequívocos para hacer esta clasificación. A continuación vamos a tratar de exponer las diferentes clasificaciones que se pueden realizar en torno a los mismos. Es necesario añadir que dichas clasificaciones responden a criterios diferentes y en ocasiones complementarios, y además no podemos considerarlas de forma autónoma, pues al hablar de delincuencia informática en muchas ocasiones, actuaciones de un determinado sujeto puede incardinarse entre diferentes listas[344].

Lo cierto es que en la actualidad existe una concepción muy amplia de lo que pueden denominarse delitos informáticos, pero la realidad es que analizando detenidamente los diferentes tipos penales podemos discrepar en no pocos casos de la idoneidad de incorporar el adjetivo "informático" a los delitos en cuestión. Como veremos en las páginas siguientes, diferentes organismos y regulaciones realizan clasificaciones de diferente forma. Si el nexo común de todas ellas es que en algún momento del *iter criminis* aparecerá un sistema o medio informático, veremos que éste no siempre lo hace con la misma trascendencia o posición[345]. Los sistemas

[344] DÍAZ GÓMEZ, A.: "El delito…" ob. cit. pp. 181 y 182, "se han expuesto por la doctrina numerosas clasificaciones de los delitos informáticos. Desde las calificaciones más simples, como las que los dividen por su carácter económico o lucrativo y afección a la privacidad […] a las más complejas, en función del método informático utilizado para lesionar al bien jurídico en cuestión. Especial interés tiene la clasificación que diferencia si el sistema informático es el objetivo de la acción ilícita o si es tan sólo un instrumento para cometer otros delitos Por último, otra clasificación de delito informático que es importante mostrar a efectos de este trabajo es aquella que diferencia entre la criminalidad que se vuelca en Internet y aquella que se desarrolla sobre «aparatos tecnológicos» (ordenadores, teléfonos móviles, etc.)". También enumera algunas listas CRUZ DE PABLO, J. A.: *Derecho penal y nuevas tecnologías. Aspectos Sustantivos*, Ed. Grupo Difusión, 1ª edición, Madrid, 2006, pp. 21 y ss.

[345] GONZÁLEZ RUS, J. J.: "Protección…" ob. cit. (sin numerar), señalaba, con razón, antes de acabar el siglo XX que "las formas de comisión posibles son tantas y tan diversas y las figuras delictivas que pueden verse implicadas tan distintas (hurto, robo, estafa, daños, falsificaciones, descubrimiento de secretos de empresa, utilización ilegítima de terminales de telecomunicación, defraudaciones de la propiedad intelectual, etc.) que los intentos de clasificación resultan particularmente complicados". Desde una perspectiva policial lo intenta LÓPEZ, A.: "La investigación policial en Internet: estructuras de cooperación internacional" en *Revista de Internet, derecho y*

informáticos o la información contenida en ellos en general pueden encuadrarse en dos listas diferenciadas: como medios para cometer delitos o, por el contrario, como objetos de las acciones delictivas[346]. Con base en esta diferencia sustancial, podremos hablar de delitos informáticos en sentido amplio o delitos informáticos *stricto sensu*[347]. Pero como ya hemos ido viendo a lo largo del estudio, y confirmaremos a continuación, esta diferenciación básica no es la preferida por los diferentes organismos e instituciones que han manifestado su idea sobre cómo ordenar los delitos informáticos. Y no es hasta un momento sorprendentemente reciente cuando, en el caso español a través de la Fiscalía General del Estado, se ha realizado una marcada línea de separación entre unos y otros, como veremos en las próximas páginas.

a.1. Delitos informáticos según establece la OCDE.

La Organización de Cooperación y Desarrollo Económico fue la primera organización de carácter internacional que elaboró un informe con los diferentes

política. Revista d'internet, dret i política, nº 5, 2007, pp. 64 y ss., al señalar que deben diferenciarse a través de los sujetos, por un lado piratas informáticos (que se conformaría como un gran cajón de sastre), y, por otro, aquellos relacionados principalmente con la pornografía infantil, que demuestran unas características del delincuente ampliamente diferenciadas de los primeros.

[346] ADÁN DEL RÍO, C.: "La persecución…" ob. cit. p. 152, divide los delitos informáticos en dos grandes grupos, aquellos en los que los sistemas informáticos son el medio, y aquellos delitos en los que en cambio son el objeto (pudiendo ser a la vez el medio). También TÉLLEZ VALDÉS, J.: "Delitos…" ob. cit. pp. 114 y ss.

[347] Según el grupo de expertos reunidos por la OCDE en Paris en mayo de 1993 estos serían "cualquier comportamiento antijurídico, no ético o no autorizado, relacionado con el procesado automático de datos y/o transmisiones de datos." En esa misma línea se manifiesta la UE en su comunicación COM(2000)890 final, de 26 de enero, al señalar que "se aborda la delincuencia informática en el sentido más amplio; cualquier delito que de alguna manera implique el uso de tecnología de la información, sin embargo, existen distintos puntos de vista sobre lo que constituye la delincuencia informática, suelen utilizarse indistintamente los términos delincuencia informática, delincuencia relacionada con la informática, delincuencia de alta tecnología y delincuencia cibernética. Cabe diferenciar entre los delitos informáticos específicos y los delitos tradicionales perpetrados con ayuda de la informática". También TÉLLEZ VALDEZ, J.: *Derecho informático*. Ed. Mc Graw Hill, 2ª edición, México, 1996, pp. 103 y 104, o la Instrucción 2/2011, sobre el fiscal de sala de criminalidad informática y las secciones de criminalidad informática de las fiscalías, p. 6, "no debe llevarnos sin más a considerar que cualquier conducta delictiva en cuya ejecución se haga uso de las tecnologías de la información y la comunicación ha de incluirse en la categoría que nos ocupa [delitos informáticos], pues ello daría lugar a una desnaturalización del concepto, tal y como viene siendo considerado internacionalmente, e incluso a un desbordamiento del propio planteamiento de la especialización en este ámbito".

tipos de delitos informáticos. Aunque su papel en la regulación internacional de los delitos informáticos ya lo hemos analizado en este segundo capítulo del estudio, señalamos ahora la clasificación que elaboró en su informe "Delitos de informática: análisis de la normativa jurídica" en 1986, clasificación que no ha modificado, a pesar de haber realizado sendos informes de directrices para la seguridad de sistemas y redes de información en los años 1992 y 2002.

En este informe de 1986 la OCDE estableció las que deberían ser las líneas generales de las políticas legislativas para prevenir la delincuencia informática y realizó una primera clasificación de cuáles eran las conductas que debían recogerse en las legislaciones penales. Las cinco acciones que señalaba el informe como merecedoras de reproche penal eran[348]:

1.- La introducción, alteración, borrado y/o supresión deliberada de datos informáticos y/o programas de ordenador con la intención de cometer una transferencia ilegal de fondos o de otra cosa de valor.
2.- La introducción, alteración, borrado y/o supresión deliberada de datos informáticos y/o programas de ordenador con la intención de cometer una falsificación.
3.- La introducción, alteración, borrado y/o supresión deliberada de datos informáticos y/o programas de ordenador, u otra interferencia con sistemas de ordenadores, con la intención de obstaculizar el funcionamiento de un sistema informático y de telecomunicaciones.
4.- La infracción del derecho exclusivo del titular de un programa de ordenador protegido con la intención de explotar comercialmente el programa y ponerlo en el mercado
5.- El acceso o la interceptación de un sistema informático o de telecomunicaciones producido sin conocimiento y sin la autorización de la persona responsable del

[348] OCDE: "Computer-related…" ob. cit.

sistema, ya sea: i) infringiendo las medidas de seguridad o ii) con intenciones deshonestas o dañinas[349].

Mientras que las dos primeras acciones constituyen tipos de estafas informática y falsedad, la tercera se convierte en acciones de daños informáticos, la cuarta se dirige a la protección de los derechos de propiedad intelectual o industrial y la quinta y última se relacionaría con acciones contra el secreto de las comunicaciones o la intimidad. Es importante señalar, por ahora, que si bien las acciones primera, segunda y cuarta utilizan el sistema informático como medio para conseguir sus fines delictivos, en el tercer y quinto tipo de conductas el sistema informático o su contenido se sitúan como los objetos sobre los que recae la acción delictiva.

a.2. Delitos informáticos según establece la ONU.

Durante el 8º Congreso de las Naciones Unidas para la Prevención del Delito y Justicia Penal celebrado en La Habana, Cuba, del 27 agosto a 7 septiembre de 1990[350], la Asamblea General de Naciones Unidas adoptó una resolución relativa a la legislación de delitos informáticos. Basándose en dicha resolución, en 1994 publicó un Manual de delitos informáticos que realiza la siguiente clasificación[351]:

1.- Fraude por manipulación informática: consiste en modificar los programas informáticos del sistema para conseguir un beneficio patrimonial. La manipulación puede realizarse desde sistemas ajenos, desde el mismo sistema o a través de aparatos electrónicos capaces de engañar al sistema informático atacado. En todos los casos el objetivo de las acciones es conseguir un beneficio patrimonial gracias a la manipulación.

[349] Traducción de la clasificación de la OCDE tomada de SIEBER, U.: "Documentación para una aproximación el delito informático" en MIR PUIG, S. *Delincuencia Informática*, Ed. PPU, 1ª edición, Barcelona, 1992, pp. 90 y 91.

[350] Informe general del 8º Congreso de las Naciones Unidas sobre Prevención del Delito y Justicia Penal, La Habana, Cuba, 27 de agosto a 7 de septiembre de 1990, pp. 149 y ss.

[351] ONU: "Manual de las Naciones Unidas sobre prevención y control de delitos informáticos" en *Revista Internacional de Política Criminal*, Ed. Naciones Unidas, nº 43 y 44, 1994. El texto completo del manual se puede encontrar en http://www.uncjin.org/documents/irpc4344.pdf

2.- Falsificaciones informáticas: se produce cuando se alteran de forma ilícita los documentos electrónicos. La ONU también incluye en este apartado los delitos relativos a la utilización de sistemas informáticos para realizar falsificaciones de documentos.
3.- Daños o modificaciones de programas o datos informáticos: es el acto de borrar, suprimir o modificar sin autorización datos o programas informáticos con la intención de obstaculizar el funcionamiento normal del sistema. Generalmente son producidas por virus informáticos de cualquiera de los supuestos a los que ya nos referimos en el capítulo primero.
4.- Acceso no autorizado a sistemas: gracias a las redes de comunicaciones, generalmente Internet, se trata de acceder a sistemas ajenos sin necesidad de estar físicamente presente en donde se encuentra el sistema atacado; hoy en día estas acciones están muy relacionadas con los casos de *hacking* web que ya estudiamos.
5.- Reproducción no autorizada de programas informáticos con derechos de autor: se refiere en general a la reproducción o difusión no autorizada a través de medios informáticos de programas de ordenador u otros materiales con derechos de autor.

Como se desprende de la clasificación realizada por la ONU en 1994 podemos afirmar que sigue una línea muy pareja a la realizada por la OCDE en 1986. Con descripciones algo más vagas y con una mayor vocación generalista que la clasificación anterior, parece reconocer la necesidad de regular penalmente las mismas acciones: fraudes usando ordenadores, falsificaciones, daños informáticos, accesos ilícitos y acciones que vulneran la propiedad intelectual. Por ello podemos concluir, al igual que en la clasificación anterior, que los sistemas informáticos pueden situarse en dos vertientes, aquella en la que los sistemas son el objeto sobre el que recae la acción delictiva y aquellos en los que son medios para conseguir los fines ilícitos.

a.3. Delitos informáticos según establece la Unión Europea.

En la actualidad, España, como país miembro de la Unión Europea, ve sometida su actuación legislativa a la regulación que de algunas materias se impone por parte de la Unión. Aunque ésta no ha llegado a legislar en todos los extremos en los que dispone de competencia, sí ha emitido la Comunicación de la Comisión al

Consejo, al Parlamento Europeo, al Comité Económico y Social y al Comité de las Regiones denominada "creación de una sociedad de la información más segura mediante la mejora de la seguridad de las infraestructuras de información y la lucha contra los delitos informáticos", de 26 de enero de 2001, en la que establece como orientar sus políticas legislativas respecto a los delitos informáticos y qué campos son susceptibles de regulación penal[352]:

1.- Delitos contra la intimidad: protección contra la recogida, almacenamiento, modificación, revelación o difusión de los datos personales de usuarios de sistemas informáticos.
2.- Delitos relativos al contenido: no sólo referidos a la pornografía infantil, sino también a declaraciones racistas y la información que incita a la violencia o al terrorismo.
3.- Delitos económicos, acceso no autorizado y sabotaje: dentro de este subapartado introduce un compendio de prácticas como la piratería, el sabotaje informático y la distribución de virus, el espionaje informático y la falsificación y el fraude informáticos
4.- Delitos contra la propiedad intelectual: protección jurídica de programas de ordenador y de bases de datos, violación de derechos de autor, así como persecución de programas o artilugios informáticos que ayuden a la comisión de este tipo de delitos.

Si bien es cierto que la clasificación que realiza la Unión Europea es muy general, se debe recordar que su capacidad legislativa es mucho mayor que la de las organizaciones anteriormente expuestas y en este caso, dentro de los instrumentos de los que dispone ha utilizado una mera Comunicación. Por ello, cabe esperar que según vaya profundizando en la regulación de dichas prácticas a través de Decisiones Marco o Directivas, el catalogo se vaya ampliando y pormenorizando considerablemente[353]. En todo caso la política de la Unión parece confirmar la

[352] COM(2000)890 final, de 26 de enero de 2001. El texto completo de la comunicación se puede encontrar en: http://eur-lex.europa.eu/lexuriserv/lexuriserv.do?uri=com:2000:0890:fin:es:pdf

[353] La Decisión Marco 2005/222/JAI de 24 de febrero es el máximo exponente de la regulación de la Unión Europea en materia de delitos informáticos. Sin embargo, en ella sólo se regulan las prácticas de: a) acceso ilegal a los sistemas de información, b) intromisión ilegal en los sistemas de información

tendencia de las anteriores clasificaciones, a las que añade además la categoría relativa a los delitos relacionados con el contenido (pornografía infantil principalmente), acciones que eran inéditas hasta el momento dentro del catálogo de la delincuencia informática.

a.4. Delitos informáticos según establece el Convenio sobre la Ciberdelincuencia de Budapest de 23 de noviembre de 2001.

El Convenio sobre la Ciberdelincuencia de Budapest, de 23 de noviembre de 2001, es otra de las herramientas fundamentales del Derecho internacional para la homogenización de las legislaciones penales respecto de los delitos informáticos. Habiendo ya profundizado sobre su contenido, podemos ahora señalar cuales son las conductas que entiende deben ser tipificadas en los ordenamientos penales de los países firmantes[354]:

1.- Delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos: en esta categoría engloba el acceso ilícito (no autorizado) a un sistema informático (art. 2), la interceptación ilícita de transmisiones de datos entre sistemas informáticos o dentro del mismo (art. 3), los ataques a la integridad de los datos (art. 4) o los sistemas (art. 5) y el abuso de dispositivos, es decir, la producción, venta, obtención, difusión u otra puesta a disposición de dispositivos o programas informáticos adaptados para la comisión de los delitos anteriores o de contraseñas o códigos de acceso que permitan acceder a otros sistemas informáticos (art. 6).
2.- Delitos informáticos: dentro de esta categoría se encontraría la falsificación informática (art. 7) y el fraude informático (art. 8) en la misma línea que las clasificaciones anteriores de la OCDE y la ONU.
3.- Delitos relacionados con el contenido: sanciona la producción de pornografía infantil para su distribución, la oferta, la puesta a disposición, la difusión, la

y c) intromisión ilegal en los datos. Podemos afirmar por tanto que, si bien desde la Unión Europea se ha realizado un catálogo aproximado de los delitos informáticos, sólo se ha legislado en una parte de ese ámbito. También se recogen detalladamente conductas que deben ser tipificadas como delictivas en la Directiva 2011/93/UE del Parlamento Europeo y del Consejo 13 de diciembre de 2011, relativa a la lucha contra los abusos sexuales y la explotación sexual de los menores y la pornografía infantil.

[354] El texto completo del Convenio se puede encontrar en: http://www.coe.int/t/dghl/standardsetting/t-cy/ets_185_spanish.pdf

transmisión, la adquisición o la mera posesión en o a través de sistemas informáticos (art. 9).

4.- Delitos relacionados con infracciones de la propiedad intelectual y de los derechos afines (art. 10), de forma similar a las clasificaciones anteriores.

En esta nueva clasificación destaca sobremanera el nivel de detalle y la inclusión de nuevas acciones. Aparece por primera vez como acción merecedora de reproche penal aquella relacionada con el abuso de dispositivos, que se suma a las anteriores, que además sufren una notoria restructuración y un mayor nivel de detalle en su definición. Además, en comparación con las listas anteriores, cabe destacar que la realizada en este Convenio se hace desde una perspectiva de lógica legislativa, entre otros puntos reflejada en que se estructura sobre la base de un articulado y en que apremia a los Estados a acometer las reformas oportunas en sus ordenamientos penales. La aplicación del mismo deja de ser una mera recomendación, como en el caso de la lista de la OCDE o el Manual de la ONU, o una declaración de intenciones como la Comunicación de la Unión Europea, para convertirse en una norma imperativa de Derecho internacional para aquellos países que ratifiquen el Convenio.

a.5. Delitos informáticos conforme al Código penal de 1995.

En el caso del Código penal español no existe una clasificación sobre los diferentes tipos de delitos informáticos[355], sino que se encuentran diseminados en diferentes títulos y artículos. En ellos, los sistemas informáticos o la información aparecen referidos de alguna manera que, incluso, en algunos de ellos no supone la mención explícita de los mismos.

La realidad es que podemos encontrar acciones típicas que, de una manera amplia, pueden llegar a ser relacionadas con la delincuencia informática. Así, nuestro Código penal en su redacción vigente regula[356]:

[355] HUETE NOGUERAS, J.: "La reforma…" ob. cit. p. 2, "el Código penal no contempla los delitos informáticos como categoría autónoma".

[356] De forma muy general, asociando acciones típicas con sucesos del día a día los clasifica el magistrado-juez VELASCO NÚÑEZ, E.: "La investigación de delitos informáticos con garantías judiciales: nuevos formatos para la delincuencia" en *Telos: Cuadernos de comunicación e innovación*,

1.- Delitos de abusos sexuales a menores de trece años: el artículo 183 *bis* CP tipifica explícitamente el aprovechamiento de los sistemas informáticos para contactar y concertar encuentros con menores de trece años para cometer alguno de los tipos básicos de agresión sexual (art. 178 CP), abuso sexual (art. 183 CP) o pornografía infantil (art. 189 CP).

2.- Delitos relacionados con la pornografía infantil: amen de lo establecido en el artículo 183 *bis* CP, dentro de los delitos relativos a la prostitución y a la corrupción de menores encontramos explícitamente señalado en el art. 189.1.b CP que la producción, venta, distribución, exhibición, oferta y la ayuda para realizar algunas de estas acciones será penada. Este artículo encuentra su razón de ser en la necesidad del legislador de tipificar la difusión general (sin un destinatario concreto) de pornografía infantil en las redes de comunicaciones[357].

3.- Delitos de descubrimiento y revelación de secretos: el artículo 197 CP establece como acciones típicas tanto la interceptación de e-mails o comunicaciones informáticas (art. 197.1 CP) como el acceso no autorizado a sistemas informáticos ajenos vulnerando las medidas de seguridad de éstos (art. 197.3).

4.- Delitos de robo con fuerza en las cosas: dentro de este tipo penal, se menciona expresamente en el artículo 239 CP en relación con 238.4 CP que las llaves falsas utilizadas para cometer el robo podrán ser cualquier instrumento tecnológico de eficacia similar al de una llave magnética o mando a distancia, lo que abre una gran

---

nº 85, 2010, p. 113. De forma más estricta (aunque anterior a la reforma de 2010) el mismo en VELASCO NÚÑEZ, E.: "Aspectos…" ob. cit. p. 1. Una relación de delitos informáticos más detallada se puede encontrar en CORCOY BIDASOLO, M.: "Problemática…" ob. cit. pp. 7 y ss. También (previo a la reforma de 2010), en URBANO CASTRILLO, E.: "Infracciones patrimoniales por medios informáticos y contra la información, como bien económico" en VELASCO NÚÑEZ, E. (dir.): *Delitos contra y a través de las nuevas tecnologías. ¿Cómo reducir su impunidad?*, Ed. Consejo General del Poder Judicial, Cuadernos de Derecho Judicial, 1ª edición, Madrid, 2006, pp. 159 y ss. Por último, una clasificación de los delitos informáticos desde un punto de vista ético y no jurídico-penal en MIGUEL MOLINA, M. R. y OLTRA GUTIÉRREZ, J. V.: *Deontología y aspectos legales de la informática: cuestiones éticas, jurídicas y técnicas básicas*, Ed. Universidad Politécnica de Valencia, 1ª edición, 2007, pp. 155 y ss.

[357] Hasta la entrada en vigor de la LO 11/1999, de 30 de abril, de reforma del Código penal, no existía en nuestro Código tal previsión penal para estos hechos, lo que llevó al archivo de causas penales en las que los acusados habían distribuido este tipo de contenido en la red, FERNÁNDEZ TERUELO, J. G.: *Cibercrimen. Los delitos cometidos a través de internet*, Ed. Constitutio Criminalis Carolina, 1ª edición, Oviedo, 2007, pp. 55 y ss.

cantidad de posibilidades de introducción de los sistemas informáticos con el objeto de perpetrar robos con fuerza, utilizando sistemas informatizados para anular las medidas de seguridad que dependan del funcionamiento correcto de otros sistemas informáticos de gestión de seguridad[358].

5.- Delitos de estafa informática: el artículo 248.2.a CP introduce la estafa a través de la manipulación informática para conseguir transferencias de activos patrimoniales en perjuicio de otro. Además en el artículo 248.2.b CP se tipifica el abuso de dispositivos en relación a este delito.

6.- Delitos de defraudaciones de fluido eléctrico: el artículo 255 CP regula, en el ámbito informático, la defraudación de telecomunicaciones, que en la actualidad mucho tiene que ver con la distribución ilegal de canales de televisión de pago. Además el artículo 256 castiga específicamente el uso no consentido de terminales de comunicación[359].

7.- Delitos de daños informáticos: también conocido como sabotaje informático, el actual artículo 264 CP regula tanto los daños sobre datos, programas informáticos o documentos electrónicos (art. 264.1 CP), como la interrupción u obstaculización de sistemas informáticos en su conjunto a través de la manipulación de sus datos informáticos (art. 264.2 CP).

8.- Delitos contra la propiedad intelectual: se tipifican detalladamente las conductas típicas que vulneran los derechos de propiedad intelectual, especialmente aquellas destinadas a la difusión, sin importar el medio empleado (art. 270.1 CP). Además se tipifica el abuso de dispositivos destinados a facilitar la supresión o neutralización de los sistemas anticopia de las obras (que generalmente serán programas de ordenador).

---

[358] Véase el ejemplo en que un experto en cajas fuertes electrónicas que conecta su ordenador al sistema informático que gestiona la caja fuerte, y gracias a sus conocimientos consigue que la puerta se abra como si hubiese sido introducida la clave correcta sin que esto haya realmente ocurrido.

[359] FARALDO CABANA, P.: "Defraudación de telecomunicaciones y uso no consentido de terminales de telecomunicación. Dificultades de delimitación entre los arts. 255 y 256 CP" en MUÑOZ CONDE, F., LORENZO SALGADO, J. M., FERRÉ OLIVÉ, J. C., BECHIARELLI, E. C. y NÚÑEZ PAZ, M. Á. (dirs.): *Un Derecho penal comprometido. Libro homenaje al Prof. Dr. Gerardo Landrove Díaz*, Ed. Tirant lo Blanch, 1ª edición, Valencia, 2011, pp. 363 y ss.

9.- Delitos relativos al mercado y a los consumidores, concretamente de descubrimiento de secretos de empresa: en el artículo 278 CP, en la línea del artículo 197 CP pero en el ámbito empresarial, se tipifica el apoderamiento de secretos de empresa a través de cualesquiera medios, contenidos en soportes informáticos, de datos o documentos electrónicos.

10.- Delitos contra los servicios de radiodifusión e interactivos: previstos y penados en el artículo 286 CP, que a menudo se incluyen dentro de los delitos de propiedad intelectual[360]. En concreto, la actual redacción introduce, en sus apartados segundo y cuarto, los delitos de alteración y duplicación del número identificativo de equipos de telecomunicaciones, su comercialización y su utilización. El abuso de dispositivos para cometer estas acciones también se encuentra previsto y penado en ese mismo artículo[361].

Como ya se ha señalado, el listado de delitos en los que pueden aparecer los sistemas informáticos en la actualidad es muy amplio. Así, no podemos olvidar, sin haber sido incluidos en la lista anterior, algunos ejemplos: a) en los delitos de amenazas (arts. 169, 170 y 171 CP) viene siendo recurrente la utilización de sistemas informáticos para procurarse el anonimato y por la facilidad que le supone al autor localizar a la víctima; b) también han venido utilizándose los medios informáticos en el delito de provocación sexual (art. 186.2 CP) que tipifica la difusión por cualquier medio de material pornográfico entre menores de edad o incapaces; c) igualmente el artículo 211 CP establece que en los delitos de injurias y calumnias hechos con publicidad (donde se agrava la pena) se entenderá por publicidad hacerlo por medio de imprenta, radiodifusión u otro de eficacia semejante, siendo en este caso común la utilización de medios informáticos (redes sociales); d) también en nuestra regulación penal, los artículos relativos a las falsedades en documento público y privado (arts.

[360] MATA y MARTÍN, R. M.: "Protección penal de la propiedad intelectual y servicios de radiodifusión e interactivos: excesos y equívocos. Su continuación en la reforma de 25 de noviembre de 2003" en CARBONELL MATEU, J.C., DEL ROSAL BLASCO, B., MORILLAS CUEVA, L., ORTS BERENGUER, E. y QUINTANAR DÍEZ, M. (coords.): *Estudios penales en homenaje al profesor Cobo del Rosal*, Ed. Dykinson, 1ª edición, Madrid, 2006, pp. 619 y ss.

[361] MOYA FUENTES, M. M.: "La alteración y duplicación del número identificativo de equipos de telecomunicaciones, su comercialización y su utilización: art. 286.2 y 4 CP" en *Revista Electrónica de Ciencia Penal y Criminología*, nº 11-2, 2009: http://criminet.ugr.es/recpc/11/recpc11-02.pdf

390 a 400 bis CP) son susceptibles de ser cometidos por medios informáticos, o bien pueden ser precisamente documentos electrónicos el objeto de falsificación, y también se castiga de forma específica la tenencia (entre otros instrumentos) de programas de ordenadores destinados a realizar los delitos de falsedad en documentos; e) puede aparecer la utilización de sistemas informáticos en los delitos cometidos contra las instituciones del Estado (art. 492 a 505), especialmente en aquellos casos en que se afecte a los sistemas informáticos que utilizan estas instituciones, y como consecuencia de ello se vea afectado el normal desarrollo de sus funciones[362] y f) en la línea de lo que ocurre con las injurias y calumnias, se castiga también la publicidad (difusión) en el delito de genocidio de ideas que justifiquen este tipo de delitos (art. 607.2 CP).

Se desprende de esta amplísima -y no cerrada- clasificación que la utilización de sistemas informáticos provoca, por un lado la aparición de nuevos delitos (daños informáticos del artículo del artículo 264 CP o acceso ilícito a sistemas informáticos del 197.3 CP) y por otro, en la mayoría de los casos, un considerable aumento de la casuística de delitos que ya existían en nuestro ordenamiento penal. Podemos señalar, como ya se ha realizado con anterioridad, que si bien todas estas conductas son denominadas hoy por la doctrina "delitos informáticos", tal concepto es demasiado amplio y en muchas ocasiones la única relación con la informática es la aparición, en algún momento de la comisión del delito, de un sistema informático.

a.6. Delitos informáticos conforme a la clasificación de la Fiscalía General del Estado en España.

Precisamente sobre la falta de concreción con que se utiliza la expresión "delitos informáticos" se ha pronunciado en España la Fiscalía General del Estado en la Instrucción 2/2011, del Fiscal de Sala de criminalidad informática y las secciones

[362] Aunque no se ha dado el caso en la realidad española y por tanto no existe pronunciamiento jurisprudencial al respecto (tampoco se ha pronunciado la doctrina) cabría preguntarse si el artículo 497, que tipifica la perturbación de las sesiones de Congreso de los Diputados, Senado o Asamblea Legislativa de Comunidad Autónoma puede cometerse hoy en día a través de medios informáticos, ya sea introduciéndose en los sistemas informáticos de la institución o bloqueando con un ataque informático su funcionamiento, de tal forma que sistemas tales como los de votación o comunicación queden inutilizados. Por otro lado, los delitos de injurias y calumnias contra las instituciones del Estado encuentran de nuevo en la informática un medio idóneo para ser cometidas.

de criminalidad informática de las Fiscalías, en la que realiza una nueva clasificación, precisamente intentando diferenciar los delitos informáticos en sentido estricto, de aquellos otros delitos en los que la informática simplemente aparece de forma incidental[363].

En este sentido, la citada Instrucción señala que tras el Convenio sobre la Ciberdelincuencia de Budapest, de 23 de noviembre de 2001, "es, por tanto, el momento oportuno de reforzar la unidad de actuación del Ministerio Fiscal también en esta materia completando, al tiempo, el sistema de especialidades del que se ha ido dotando la Institución para el eficaz cumplimiento de las funciones que constitucionalmente le han sido encomendadas"[364]. A partir de estas premisas básicas, la Instrucción hace una nueva clasificación de los delitos informáticos (en sentido amplio) recogidos en nuestro texto penal. Esta nueva clasificación parte de la idea de eficacia a la hora de investigar los hechos constitutivos de delitos informáticos desde un prisma eminentemente práctico[365]:

1.- Delitos en los que el objeto de la actividad delictiva son los sistemas informáticos o las TICs: son los delitos propiamente informáticos. Para la Fiscalía estos son los daños informáticos del artículo 264 CP; el acceso ilícito a sistemas informáticos del

[363] La Memoria de la Fiscalía del año 2012, en cuanto a las actividades relacionadas con delitos informáticos, recuerda que ya en 2007 existía una serie de desajustes en la forma de tramitar los procedimientos relativos a la delincuencia informática entre diferentes Fiscalías provinciales al no existir clasificación ni procedimiento unificado sobre los delitos informáticos: "como ya se ha puesto de manifiesto, a partir del año 2007 fueron muchas las Fiscalías en las que se encomendó específicamente a alguno de los Fiscales de la plantilla la coordinación de los procedimientos relativos a conductas susceptibles de encuadrarse en este apartado, pero ni ello era así en todos y cada uno de los órganos provinciales ni, por otra parte, se encontraba definido con carácter general el contenido y alcance de esta función, por lo que el trabajo desarrollado por los encargados de esta materia en los diversos territorios podía diferir y de hecho presentaba variaciones importantes entre unas Fiscalías y otras". Memoria de la Fiscalía General del Estado 2012 p. 1114.

[364] Instrucción 2/2011, sobre el Fiscal de Sala de criminalidad informática y las secciones de criminalidad informática de las Fiscalías, p. 5.

[365] La Instrucción 2/2011, sobre el Fiscal de Sala de criminalidad informática y las secciones de criminalidad informática de las Fiscalías, p. 6, precisa que "exigencias mínimas de operatividad y eficacia demandan, por tanto, una mayor concreción en la delimitación del objeto de actividad en esta área de trabajo de tal forma que únicamente alcance su competencia, cuando, en los indicados supuestos, la utilización de dichas tecnologías resulte ser determinante en el desarrollo de la actividad delictiva y/o dicha circunstancia implique una elevada complejidad en la dinámica comisiva y, en consecuencia, una mayor dificultad en la investigación del hecho e identificación de sus responsables".

artículo 197.3 CP, así como los delitos del artículo 197.1 CP y 197.2 CP sólo cuando el descubrimiento y revelación bien se realice utilizando sistemas informáticos para realizar el descubrimiento o bien recaiga sobre datos que se hallen registrados en ficheros o soportes informáticos; el delito de descubrimiento y revelación de secretos de empresa previstos y penados en el artículo 278 CP cuando sean cometidos a través de sistemas informáticos, o cuando los datos objetos del delito se hallen igualmente en sistemas informáticos y los delitos contra los servicios de radiodifusión e interactivos previstos y penados en el artículo 286 CP.

2.- Delitos en que la actividad criminal se sirve para su ejecución de las ventajas que ofrecen las TICs.: Delitos de estafa previstos y penados en el artículo 248.2 CP, siempre que, en los supuestos a) y c) se utilicen los sistemas informáticos para llevar a efecto la transferencia u operación en perjuicio de otro; delitos de acoso a menores de 13 años, previstos y penados en el art. 183 *bis* CP cuando se lleve a efecto a través de la sistemas informáticos; delitos de corrupción de menores o de personas discapacitadas o relativas a pornografía infantil o referida a personas discapacitadas del artículo 189 CP cuando para el desarrollo o ejecución de la actividad delictiva se utilicen las sistemas informáticos y delitos contra la propiedad intelectual de los artículos 270 y siguientes del CP cuando se cometan utilizando las sistemas informáticos.

3.- Delitos en los que la actividad criminal, además de servirse para su ejecución de las ventajas que ofrecen las TICs, entraña tal complejidad en su investigación que demanda conocimientos específicos en la materia: además de cualesquiera de los anteriores, especialmente los delitos de falsificación documental (arts. 390 CP y siguientes) cuando para la ejecución del delito se hubieran empleado sistemas informáticos; delitos de injurias y calumnias contra funcionario público, autoridad o agente de la misma (arts. 211 CP y siguientes) cometidos a través de las sistemas informáticos; delitos de amenazas y coacciones (arts. 169 CP y siguientes); delitos contra la integridad moral (art. 173.1 CP) cometidos a través de sistemas informáticos y delitos de apología o incitación a la discriminación, el odio y la violencia o de negación o justificación de los delitos de genocidio (arts. 510 CP y 607.2 CP). Todos ellos siempre que la utilización de sistemas informáticos fuera

determinante en la actividad delictiva y generara especial complejidad en la investigación criminal. Además, cualquier otro tipo delictivo en cuya ejecución haya sido igualmente determinante la utilización de los sistemas informáticos se encuadraría en esta lista.

B) EL OBJETO CONCRETO DE NUESTRO ESTUDIOS. LOS DAÑOS INFORMÁTICOS

Es obvio, aunque importante, señalar que no todas las acciones antes descritas suponen un delito de daños informáticos. Como hemos visto, tanto el Código penal, como el resto de organismos internacionales describen una multitud de acciones delictivas en las que participa la informática al margen de los daños informáticos, cuyo estudio excede las aspiraciones de la presente investigación. En la segunda y tercera parte de esta investigación realizaremos el estudio jurídico penal en torno a la regulación de los daños informáticos en nuestro Código penal y plantearemos los problemas que en la actualidad plantea la regulación vigente, así como una propuesta para superar las deficiencias detectadas.

Los daños informáticos, o sabotaje informático, se encuentran regulados principalmente en nuestro Código penal en el artículo 264[366]. En el mismo encontramos las acciones relacionas con el daño sobre datos, programas informáticos y documentos electrónicos, así como acciones de interrupción y obstaculización de sistemas informáticos en su conjunto, además de una serie de circunstancias agravantes específicas y otras consideraciones especiales. Podemos afirmar, por tanto, que nos encontramos ante dos tipos penales diferentes, ambos de daños informáticos.

El artículo 264.1 CP castiga el daño (en sentido amplio) sobre datos, programas informáticos y documentos electrónicos. Precisamente el objetivo general de los tipos de virus que ya analizamos es provocar este resultado, por lo que al detenernos en su estudio veremos qué papel tienen en la comisión del delito los sujetos que crean o distribuyen estos virus. El artículo 264.2 CP, al que también

[366] Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal en la redacción realizada por la LO 5/2010 de 22 de junio, de reforma del Código penal.

dedicaremos un extenso análisis, penaliza las acciones que obstaculizan o interrumpen el funcionamiento de un sistema informático. No debemos olvidar con base en los conceptos ya expuestos que un servidor donde se encuentra alojada una página web o un servicio online a los que se accede a través de una conexión a Internet no dejan de ser, en sí mismos, sistemas informáticos y que precisamente las acciones de *hacking* web pretenden en algunos casos la obstaculización o la interrupción de los mismos y, por tanto, pueden encontrar acomodo en este segundo delito de daños informáticos. En términos muy generales podemos afirmar que en la actualidad el delito del artículo 264.1 CP persigue principalmente acciones relacionadas de los virus informáticos (aunque no exclusivamente) y el delito del artículo 264.2 CP persigue las acciones relacionadas con el bloqueo de páginas webs y otros sistemas informáticos (tampoco de forma exclusiva). Sin embargo, aunque suponga adelantar algunas cuestiones a analizar, veremos que las prácticas anteriores no son las únicas que van a ser penalizadas como daños informáticos en nuestro ordenamiento, esto es, no agotan las posibilidades de los delitos de daños informáticos. Descubriremos que el legislador, por la forma de redactar los tipos, ha incluido otra serie de prácticas que pueden dar lugar igualmente a la aparición a la responsabilidad penal por daños informáticos. Precisamente en esta línea analizaremos cómo no todos los sujetos activos participantes en estos delitos tienen porque ser grandes conocedores de las técnicas informáticas existentes.

No debemos olvidar señalar que tanto los daños imprudentes (artículo 267 CP) como de la falta de daños (artículo 625.1 CP), ambos sin una regulación específica en el Código penal en relación a los datos y sistemas informáticos[367], también se encuentran tipificados y a ellos dedicaremos igualmente unas líneas en la segunda parte de esta investigación para verificar su acomodo, o no, a las particularidades de los daños informáticos del artículo 264 CP.

[367] Tanto el tipo imprudente como la falta se refieren a los delitos de daños en general, lo que, como será analizado en su momento, puede plantear problemas sobre la tipicidad de determinadas conductas realizadas sobre datos o sistemas informáticos.

SEGUNDA PARTE:

LOS DELITOS DEL ARTÍCULO 264 DEL CÓDIGO PENAL. REGULACIÓN DE LOS DAÑOS INFORMÁTICOS EN ESPAÑA

CAPÍTULO TERCERO: ANÁLISIS JURÍDICO-PENAL DE LOS TIPOS DE DAÑOS INFORMÁTICOS DEL ARTÍCULO 264 DEL CÓDIGO PENAL

1. INTRODUCCIÓN

En este capítulo la investigación se va a centrar casi exclusivamente en el artículo 264 del Código penal. En primer lugar se hará referencia a su origen y su reciente reforma para, a continuación, realizar el análisis de los tipos penales referidos a los daños informáticos tal y como han quedados redactados en el ordenamiento vigente[368]. Abordaremos de forma concreta los aspectos jurídico formales de la regulación de los daños informáticos en nuestro Código penal. El nudo de este capítulo pretende dar una visión general sobre la nueva tipificación que los daños informáticos encuentran en la legislación española. Todo ello servirá para, en la tercera parte de la investigación, poder realizar una evaluación de la misma y, en su caso, una propuesta de reforma.

Con la entrada en vigor de la LO 5/2010 de 22 de junio se han operado cambios sustanciales en la forma de tipificar las conductas referidas, hecho que nos obliga a un nuevo análisis de la situación. La redacción actual del artículo 264 del Código penal ha conseguido una regulación más precisa que la anteriormente existente, además de incluirse un nuevo tipo penal, el del apartado segundo, novedoso en nuestro ordenamiento[369]. Por tanto, quedan diferenciados dos comportamientos que el legislador ha entendido necesario regular de forma conjunta, coincidentes en algunos de sus elementos típicos, así como en las condiciones para la aparición de supuestos agravados. También se han recogido una serie de

[368] Texto del artículo desde la entrada en vigor de la LO 5/2010 de 22 de junio, que modifica sustancialmente la anterior regulación.

[369] La doctrina se muestra unánime al determinar que la evolución debe ser valorada positivamente. Por todos GÓMEZ MARTÍN, V.: "Sabotaje informático, 'top manta', importaciones paralelas y fraude de inversores: ¿algunos exponentes de un nuevo derecho Penal económico?" en *Revista Jurídica de Catalunya*, nº 4, 2011, p. 2. Sin embargo, como se verá lo largo de los siguientes capítulos, una cosa es valorar positivamente la evolución, y otra compartir en el detalle la forma en que han quedado redactados los tipos penales.

circunstancias agravantes para los delitos de los dos primeros apartados del artículo 264 del Código y, como en muchos otros preceptos a raíz de la reforma penal de 2010, se ha incluido la responsabilidad penal de las personas jurídicas cuando realizan las conductas típicas descritas[370].

Además, a diferencia de la regulación precedente, ahora las conductas descritas no suponen un supuesto agravado de los daños comunes como parecía desprenderse de la redacción anterior[371], sino que se configuran como verdaderos tipos específicos de daños que, como se verá cuando hablemos de las consecuencias jurídicas, establecen una penalidad sustancialmente más elevada en comparación con la establecida para los daños constitutivos del tipo básico de daños del artículo 263.1 CP[372].

[370] La regulación precedente situaba el delito de daños informáticos en el artículo 264 CP, en el cual se introducían en su apartado primero los supuestos agravados de daños clásicos, y en el que se reservaba el segundo apartado para los daños informáticos que, aunque con otra redacción, recogía las conductas del actual 264.1 CP. El nuevo supuesto del actual 264.2 CP, así como los tipos agravados de daños informáticos no existían hasta la reforma de 2010, al igual que la posibilidad de la imputación de tales conductas a personas jurídicas.

[371] Sobre esta cuestión ha existido siempre cierta discusión doctrinal y discrepancias en la interpretación de los tribunales que, en ocasiones, entendían que no era necesario el límite de 400 euros que se exigía en el anterior tipo básico, lo que producía la duda de si nos encontrábamos ante un tipo específico con una ubicación manifiestamente mejorable o bien ante un tipo agravado con un carácter muy especial pues no era necesaria la concurrencia de todos los elementos del tipo básico para la aparición de la modalidad agravada. A este problema se refiere DE LA MATA BARRANCO, N. J.: "El delito de daños a datos, programas, documentos y sistemas informáticos" en JUANES PECES, Á (dir.): *Reforma del Código Penal. Perspectiva Económica tras la entrada en vigor de la LO 5/2010 de 22 de junio. Situación jurídico-penal del empresario,* Ed. El Derecho, 1ª edición, Madrid, 2010, pp. 164 y 165. No son muchos los casos tratados por la jurisprudencia, baste señalar como ejemplos la SAP Barcelona 72/2008 de 18 enero, donde se entiende que "los daños informáticos son daños cualificados que tienen una naturaleza delictiva con independencia del importe de su reparación" en contraposición con la SJP nº 1 de Terrassa 20/2006 de 1 febrero donde se establece que "no ha quedado probado por ningún tipo de prueba practicada, que los daños causados asciendan a 400 euros , límite necesario para deslindar la falta del delito, elemento típico fundamental que no puede darse por supuesto".

[372] MIRÓ LLINARES, F.: "Delitos informáticos: Hacking. Daños" en ORTIZ DE URBINA GIMENO, Í. (coord.): *Memento Experto. Reforma Penal*, Ed. Ediciones Francis Lefebvre, 1ª edición, Madrid, 2010, p. 157.

2. ORIGEN Y EVOLUCIÓN DEL DELITO DE DAÑOS INFORMÁTICOS EN ESPAÑA

La introducción en el ordenamiento penal de nuevas formas delictivas suscita siempre incógnitas[373]. La relevancia que supone la superación adecuada de estos problemas se debe a que el Derecho penal, como parte del Derecho público[374], siempre se ha encontrado vinculado de manera muy estrecha con la limitación de los Derechos fundamentales de los ciudadanos[375], lo que hace necesario una correcta formulación de las conductas penalmente típicas. La regulación de los daños informáticos en nuestro ordenamiento ha supuesto una prueba para el legislador nacional en su introducción en el ordenamiento penal en 1995, así como una muestra de adaptación al espacio europeo en 2010. Ya se ha señalado que la primera regulación que de los mismos se realizó en nuestro país se produjo con la entrada en vigor del Código penal de 1995, en el que el antiguo artículo 264.2 CP señalaba como autor de un delito de daños al que por destruyera, alterara, inutilizara, o de cualquier otro modo dañara los datos, programas informáticos o documentos electrónicos ajenos contenidos en redes, soportes o sistemas informáticos. La actual regulación, que es heredera en muchos aspectos de esta primera versión[376], ocupa

[373] El propio preámbulo de la LO 5/2010 de 22 de junio, de reforma del Código penal, se expresa en esa línea al resolver que "la progresiva conquista de niveles de bienestar más elevados no es concebible, en un marco jurídico de respeto a los derechos fundamentales, sin un paralelo avance en materia de libertad y de seguridad".

[374] Por todos, ROXIN, C.: *Derecho Penal. Parte General. Tomo I*, Ed. Thomson Civitas, Navarra, 1997 (reimpresión de 2008), p. 43.

[375] En el ámbito de nuestra investigación relacionada con los delitos informáticos, LEZERTUA RODRÍGUEZ, M.: "El Proyecto…" ob. cit. p. 86 justifica que "el derecho penal es uno de los instrumentos, tal vez el más importante, de los que dispone el Estado para regular la convivencia entre particulares, determinándose, a través de él, qué comportamientos resultan inaceptables en cada comunidad humana y las sanciones que corresponde aplicar a quienes incurran en tales comportamientos, en especial aquellos que resulten lesivos de los derechos fundamentales de los demás ciudadanos".

[376] Principalmente es coincidente su ubicación en el Código, como un tipo de daño patrimonial y también se mantienen los medios comisivos ("cualquier medio" dice tanto la regulación derogada como la vigente). Además algunas acciones típicas se han mantenido con la actual redacción. Aun así se puede afirmar que ha sufrido un cambio importante como señala BARRIO ANDRÉS, M.: "El régimen jurídico de los delitos cometidos en Internet en el derecho español tras la reforma penal de 2010", en *Delincuencia informática. Tiempos de cautela y amparo,* Ed. Thomson Reuters Aranzadi, 1ª edición, Navarra, 2012, p. 44, sin obviar, como el mismo autor ha señalado también en BARRIO ANDRÉS, M.: "La ciberdelincuencia en el Derecho español" en *Revista de las Cortes Generales*, nº 83, 2011, p. 302,

actualmente todo el artículo 264 CP, y su razón de ser responde esencialmente al mandato internacional: por un lado el Convenio sobre la Ciberdelincuencia celebrado en Budapest en 2001, y por otro la, de momento vigente, Decisión Marco 2005/222/JAI del Consejo.

Por ello, antes de dar paso al análisis jurídico penal de los delitos de daños informáticos según quedan establecidos con la actual regulación, vamos a introducir este capítulo tercero con una breve referencia al origen de dicho artículo en nuestro ordenamiento y al desarrollo legislativo llevado a cabo en nuestras instituciones como consecuencia del mandato de la Unión Europea[377].

A) PRECEDENTES DE LA REGULACIÓN DE DAÑOS INFORMÁTICOS EN ESPAÑA: EL ANTIGUO 264.2 CP

La primera vez que nuestra regulación penal tipifica expresamente como delito el ataque a elementos lógicos informáticos (datos, programas informáticos o documentos electrónicos) produciendo su daño de alguna manera (destrucción, alteración o inutilización) es con la entrada en vigor del Código penal de 1995. Aunque no existe jurisprudencia al respecto que pueda aportar luz, antes de este momento los daños informáticos deberían haberse reconducido a la vía civil, ya que parece complicado encontrar cabida en los delitos de daños del Código de 1973[378].

En todo caso, la primera cuestión, a la que ya hemos hecho referencia, es que la regulación de esta figura en nuestro país llegó prácticamente con una década de retraso respecto del fenómeno tipificador de los países de nuestro entorno. Es cierto,

---

que "la reforma puede ser calificada de insuficiente y, quizás, como operación de *restlying*. El legislador sigue desconociendo la singular importancia que tienen los sistemas de información".

[377] Decisión Marco 2005/222/JAI del Consejo de 24 de febrero, HUETE NOGUERAS, J.: "La reforma…" ob. cit. p. 1.

[378] Los daños, regulados hasta entonces en los artículos 557 CP y siguientes, de forma muy parecida a como se encuentran regulados en el actual 263 CP, entendían como fundamento básico para la apreciación del delito la materialidad de la cosa. La previsión de objetos inmateriales excedía de los límites interpretativos del precepto, a pesar de voces en la doctrina que entendían que nada impedía que el objeto fuera inmaterial, por cuanto el tipo penal del artículo 557 CP no lo establecía como elemento típico, así, GONZÁLEZ RUS, J. J.: "Tratamiento…" ob. cit. pp. 12 y 13, "estimo que la materialidad de la cosa debe ser entendida en sentido diverso de la aprehensibilidad que requieren los delitos de apoderamiento, debiendo insistirse en la capacidad del objeto [informático] para ser dañado o destruido".

en todo caso, que la iniciativa política de principios de la década de 1990 pretendía la realización de un nuevo Código penal en toda su extensión, y si bien en el Anteproyecto de 1992 no existía previsión al respecto[379], el de 1994 (ambos, a la postre, bases básicas del Código de 1995) ya recogía en su texto la tipificación de las conductas de daños informáticos[380], lo que explica, en parte, la demora de nuestro legislador en acometer la necesaria introducción del tipo penal.

Pero, aparte de esta demorada aparición de tales conductas en nuestro ordenamiento penal, también podemos señalar como, al menos curioso, el hecho de que con la existencia ya contrastada de las listas de delitos informáticos ofrecidas por la OCDE en 1986, del Consejo de Europa en 1989 o de la ONU primero en 1990 y más tarde con la clasificación del Manual de 1994[381], el legislador de 1995 decidiese realizar una tipificación laxa de estas conductas en nuestro Código penal. Así, de dichas clasificaciones internacionales se desprende la necesidad de proteger tanto la integridad de datos y programas informáticos, como el funcionamiento de los sistemas informáticos de ataques que los obstaculicen. Es decir, ya en las primeras clasificaciones de delitos informáticos parece existir una dualidad en tanto en cuanto al objeto de protección: el daño a sus elementos lógicos por un lado y la obstaculización del funcionamiento de sistemas informáticos por otro. Incluso la escasa doctrina que en España se había dedicado al estudio de estos aspectos se había manifestado en este sentido de la dualidad de acciones[382].

Sin embargo, tales listados sólo pueden ser considerados como sugerencias provenientes de diferentes ámbitos, lo que no implica, y no lo hizo, una determinación en la forma de tipificar las conductas del legislador de 1995. Así, el texto finalmente aprobado señalaba como acciones típicas el daño informático en su versión más concreta, el que se produce sobre datos, programas informáticos y documentos electrónicos, dejando fuera de la regulación penal, la obstaculización de

[379] AIDP: "Computer Crime…" ob cit. pp. 567 y ss.

[380] HEREDERO HIGUERAS, M.: "Los delitos informáticos en el proyecto de código penal de 1994" en *Informática y derecho. Revista iberoamericana de derecho informático*, nº 12, 13, 14 y 15, 1996, p. 1185 y ss.

[381] Todas ellas han sido objeto de estudio en la primera parte de esta investigación.

[382] ROMEO CASABONA, C. M.: *Poder Informático y Seguridad Jurídica*, Ed. Fundesco, 1ª edición, Madrid, 1988, pp. 176 y ss. o GUTIÉRREZ FRANCÉS, M. L.: *Fraude…* ob. cit.

sistemas informáticos[383]. Por lo demás, cuando estudiemos la regulación consecuencia de la reforma de 2010, que ha venido a completar la de 1995, analizaremos, punto por punto, tanto los elementos coincidentes con la anterior, como los nuevos aspectos introducidos, pudiéndose interpretar los elementos previos a la reforma de 2010, esencialmente, de la misma forma que en la regulación actual.

B) LA REFORMA DE LOS DAÑOS INFORMÁTICOS DE 2010

Como hemos señalado, la regulación penal de daños informáticos vigente en nuestro ordenamiento jurídico ha sido ampliamente modificada con la entrada en vigor de la LO 5/2010 de 22 de junio, de reforma del Código penal, producto de la cual, principalmente, se han añadido acciones, se han sustituido algunos elementos, y se ha ampliado el catálogo de conductas punibles[384]. Es necesario precisar que la nueva regulación no se produce como un interés exclusivo del legislador en reformar las conductas punibles de daños informáticos, sino que se engloba en un proyecto mucho más ambicioso, de revisión de una gran cantidad de preceptos del Código penal.

b.1. La reforma desde el punto de vista legislativo. Cuestiones generales.

Es importante destacar, como ha señalado la doctrina, que un buen anteproyecto de ley se hace necesario si queremos conseguir que al final de todo el

[383] En algunos casos, la interpretación jurisprudencial del antiguo 264.2 CP ha sido capaz de superar este déficit, sin embargo, lo hacía desde el prisma de que a la obstaculización le precedía un daño informático de los tipificados en el antiguo artículo 264.2 CP, lo que creaba importantes lagunas, pues no toda obstaculización de un sistema informático tenía porque realizarse destruyendo, alterando o inutilizando datos informáticos. Para DE LA MATA BARRANCO, N. J, y HERNÁNDEZ DÍAZ, L.: "El delito de daños informáticos. Una tipificación defectuosa" en *Estudios penales y criminológicos*, nº 29, 2009, p. 331, "tal vez con la creación del art. 264.2 se pretende simplemente colmar lagunas de penalidad", pero que supuso una regulación rápida en la que "no se tuvo información suficiente para reflexionar sobre lo que había que proteger".

[384] A pesar de ello, se encuentran voces críticas sobre la misma, URBANO CASTRILLO, E.: "Los delitos informáticos tras la reforma del CP de 2010" en *Delincuencia informática. Tiempos de cautela y amparo*, Ed. Thomson Reuters Aranzadi, 1ª edición, Navarra, 2012, p. 21, cuando señala que la reforma "ha mejorado [la situación anterior] pero puede sostenerse, sin duda alguna, que la reforma ha defraudado las expectativas existentes" y p. 29, en la que concluye que "se ha perdido la oportunidad de establecer una regulación correcta de tan importante fenómeno delictivo" afirmando que "no basta con seguir modificando tipos penales existentes e incluyendo nuevos delitos. Se requiere una regulación general, que no tiene por qué ser muy extensa". En el mismo sentido en URBANO CASTRILLO, E.: "Los delitos informáticos tras la reforma del CP de 2010" en *Revista Aranzadi Doctrinal*, nº 9, 2010, pp. 163 y ss.

proceso se pueda obtener una buena ley tanto desde el punto de vista de técnica legislativa, como desde el punto de vista material del propio contenido de la ley. O dicho de otro modo, va a resultar extremadamente complicado que de un mal anteproyecto de ley se derive finalmente una buena ley, pues todo el proceso de tramitación, lejos de corregir los defectos de base del mismo, probablemente contribuya a aumentarlos[385]. En el caso de los daños informáticos ha sido constatable tal afirmación, pues es precisamente en el anteproyecto donde se plasma la estructura y límites de la normativa finalmente aprobada[386].

Como toda elaboración legislativa, ésta debe tener en su origen una voluntad que la promueva con la finalidad de obtener un resultado deseado[387]. Con la configuración del actual sistema de elaboración de leyes en nuestro país, dicha voluntad aparece íntimamente ligada a dos planos: el primero relacionado con el programa de gobierno del Ejecutivo (que encuentra estabilidad gracias al apoyo de la

[385] De esta opinión es GARCÍA-ESCUDERO MÁRQUEZ, P.: *Manual…* ob. cit. p. 49; o GARRIDO MAYOL, V.: *Las garantías del procedimiento prelegislativo: la elaboración y aprobación de los proyectos de ley*, Ed. Tirant lo Blanch, 1ª edición, Valencia, 2010, p. 47.

[386] Para conocer de forma apropiada a qué nos referimos por fase prelegislativa es importante establecer los momentos entre los cuales transcurre. En el caso de la elaboración de la legislación penal, como en cualquier otra ley estatal, el momento procedimental en el que se inicia el anteproyecto viene reglado en la Ley 50/1997, de 27 de noviembre, del Gobierno, la cual en su articulado, desarrollando el mandato constitucional de los artículos 87 y 88 de la Constitución, establece las pautas básicas del procedimiento de aprobación de los proyectos de ley, y en menor medida la forma de elaborar los anteproyectos de ley. Así se determina que, como requisitos necesarios para la aprobación del proyecto del ley en el Consejo de Ministros y su posterior remisión al Congreso o al Senado, es necesario que el anteproyecto de ley vaya acompañado de su correspondiente memoria, de los estudios o informes sobre la necesidad y oportunidad del mismo, un informe sobre el impacto por razón de género de las medidas que se establecen en el mismo, y una memoria económica que contenga la estimación del coste a que dará lugar. A todo ello además se deberá adjuntar el informe de la Secretaria General Técnica del Ministerio promotor (Art. 22.2 Ley 50/1997, de 27 de noviembre, del Gobierno) así como otros informes preceptivos emitidos por otros órganos del Estado que deban informar sobre la modificación legislativa penal proyectada (principalmente en materia penal el Consejo de Estado y el Consejo General del Poder Judicial: el artículo 21.2 de la Ley Orgánica 3/1980, de 22 de abril, del Consejo de Estado y el artículo 108.1.f de la Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial establecen cuándo son pertinentes sus informes, cuestión en la que nos detendremos más adelante). Por último se exige el acompañamiento de una memoria del análisis de impacto normativo, introducida por el Real Decreto 1083/2009, de 3 de julio. Véanse GARCÍA-ESCUDERO MÁRQUEZ, P.: *La iniciativa legislativa del Gobierno*, Ed. Centro de estudios políticos y constitucionales, 1ª edición, Madrid, 2000 y GARCÍA-ESCUDERO MÁRQUEZ, P.: *El procedimiento legislativo ordinario en las Cortes Generales*, Ed. Centro de Estudios Políticos y Constitucionales, 1ª edición, Madrid, 2006.

[387] GARRIDO MAYOL, V.: *Las garantías...* ob. cit. pp. 39 y ss.

mayoría de los diputados presentes en el Congreso tras la celebración de las elecciones, cuestiones éstas que no vamos ahora a analizar[388]); y un segundo plano, especialmente relevante en materia penal, vinculado a la alarma social[389] creada por determinados hechos sobrevenidos durante la legislatura[390]. Se crea, por tanto, una tensión evidente entre la necesidad de vertebrar el ordenamiento según el principio de legalidad -especialmente importante en materia penal-[391] y los problemas de la realidad legislativa actual, en especial los relativos a la legislación motorizada[392]. Además, en el caso de los daños informáticos debemos destacar que la voluntad política referida no se centra en la del Gobierno de la Nación[393], pues hablamos de legislación de la Unión Europea[394], así como de la obligación contraída producto de la ratificación del Convenio sobre la Ciberdelincuencia de 2001. Es decir, la voluntad política que promueve la reforma de los delitos de daños informáticos reside tanto en un organismo supranacional -la Unión Europea- como en una convención

[388] DÍEZ RIPOLLÉS, J. L.: *La racionalidad de las leyes penales*, Ed. Trotta, 1ª edición, Madrid, 2003, pp. 44 y 45. Para un estudio detallado, se recomienda FERNÁNDEZ-MIRANDA CAMPOAMOR, A. y FERNÁNDEZ-MIRANDA CAMPOAMOR, C.: *Sistema electoral, partidos políticos y parlamento*, Ed. Colex, 2ª edición, Madrid, 2008, especialmente los capítulos V (La representación política en el Estado con Partidos) y X a XIV (El Parlamento. El sistema parlamentario de Gobierno).

[389] GUANARTEME SÁNCHEZ LÁZARO, F.: "Alarma social y Derecho penal" en ROMEO CASABONA, C. M., GUANARTEME SÁNCHEZ LÁZARO, F. y ARMAZA ARMAZA, E. J. (coords.): *La adaptación del Derecho penal al desarrollo tecnológico*, Ed. Comares, 1ª edición, Granada, 2010, pp. 53 y ss.

[390] GARCÍA-ESCUDERO MÁRQUEZ, P.: "Consideraciones sobre la iniciativa legislativa del Gobierno*"* en *Cuadernos de Derecho público*, nº 8, 1999, p. 30, hace referencia a esta bipartición, añadiendo además un tercer motivo de inicio de la vía prelegislativa en función de la imposición derivada de la firma de tratados internacionales, y especialmente del Derecho comunitario. En todo caso creemos que esta tercera vía formaría parte del programa de gobierno del Ejecutivo, pues aun cuando sea de forma general, todo programa de gobierno contiene como clausula general cumplir los compromisos alcanzados por el Estado ante los organismos internacionales, y darles traslado a su legislación nacional; caso éste de la regulación de los daños informáticos.

[391] HUERTA TOCILDO, S.: "Principio…" ob. cit. pp. 13 y ss.

[392] Expresión acuñada por primera vez por SCHMITT, C.: *Die Lage der europaische Rechtswissenschaft*, *Internat*. Ed. Univ.-Verlag, 1ª edición, Tübingen, 1950.

[393] Aunque la voluntad política sobre la forma de solucionar los problemas existentes no se origina en el Gobierno de la Nación, su papel como agente político sigue siendo importante, pues la voluntad política de iniciar la transposición internacional si es competencia exclusivamente suya; aunque por otro lado, una vez el Estado ha ratificado sus obligaciones internacionales, tal voluntad no podría tener otra orientación.

[394] HUETE NOGUERAS, J.: "La reforma…" ob. cit. p. 2, "el precepto [nuevo artículo 264 CP] viene a cumplir las específicas obligaciones contraídas por la Decisión Marco 2005/222/JAI de 24 de febrero de 2005".

internacional (Convenio de 2001), lo que incrementa los problemas sobre transposición y aplicación de dicha normativa en nuestro ordenamiento.

El artículo 9.3 de la Constitución española de 1978 garantiza entre otros el principio de legalidad y el derecho a la seguridad jurídica como valores generales del Estado de Derecho[395]. Así mismo, el artículo 25.1 de la Constitución española profundiza en dicho principio en el ámbito penal[396]. Todo Estado democrático sujeto a las reglas del constitucionalismo moderno reconoce como principio fundamental el principio de legalidad, pues de otro modo difícilmente podríamos entender que nos encontramos ante un Estado de Derecho[397]. El derecho a la seguridad jurídica se construye vinculado inevitablemente al anterior. El contenido fundamental del principio de legalidad se centra (pero no se agota) en la función de garantía de la seguridad jurídica[398], la cual opera principalmente en favor de los ciudadanos pues sabrán a qué reglas atenerse en sus actuaciones, tanto particulares como con la propia Administración[399].

El principio de legalidad encuentra especial relevancia cuando nos encontramos en materia penal, y más si cabe cuando nos encontramos ante normativas de carácter eminentemente técnico. Cuando el Estado actúa ejerciendo el poder coercitivo, debe hacerlo siempre sujeto a unas normas y unos límites, regidos fundamentalmente por el principio de legalidad, es decir, el Estado no puede actuar

[395] Art. 9.3 CE: "La Constitución garantiza el principio de legalidad, la jerarquía normativa, la publicidad de las normas, la irretroactividad de las disposiciones sancionadoras no favorables o restrictivas de derechos individuales, la seguridad jurídica, la responsabilidad y la interdicción de la arbitrariedad de los poderes públicos".

[396] HUERTA TOCILDO, S.: "Principio…" ob. cit. p. 13.

[397] MUÑOZ CONDE, F. y GARCÍA ARÁN, M.: *Derecho Penal, Parte General,* Ed. Tirant lo Blanch, 8ª edición, Valencia, 2010, p. 99

[398] HUERTA TOCILDO, S.: "El contenido debilitado del principio europeo de legalidad penal" en GARCÍA ROCA, J. y SANTOLAYA MACHETTI, P.: *La Europa de los Derechos. El Convenio Europeo de Derechos Humanos*, Ed. Centro de Estudios Políticos y Constitucionales, 2º edición, Madrid, 2009, p.513.

[399] RODRÍGUEZ MOURULLO, G.: "El Derecho penal: paradigma de la codificación", en MENÉNDEZ MENÉNDEZ, A. (dir.): *La proliferación legislativa: un desafío para el Estado de Derecho*, Ed. Thomson Civitas, 1ª edición, Madrid, 2004, pp. 561 y ss., o QUINTERO OLIVARES, G.: *Parte…* ob. cit. pp. 57 y ss.

fuera de lo que la legalidad le permite hacerlo[400]. El principio de legalidad penal, conocido en la doctrina tradicional como *nullum crimen nulla poena sine lege* se configura como el principal límite al *ius puniendi* del Estado, que es mucho más que un enunciado y comporta una serie de garantías para el ciudadano que marcan los límites del poder del propio Estado[401]. Así estas garantías son enunciadas como *lex praevia, lex certa, lex scripta* y *lex stricta*[402]. Esta concepción del Derecho penal moderno encuentra su consolidación con el nacimiento del Estado liberal, y se ha mantenido casi inalterado y plenamente asumido por la comunidad internacional en la actualidad[403], si bien su construcción desde una perspectiva internacional puede considerarse de contenido más limitado o debilitado[404]. Aunque ahora no es menester entrar en un profundo análisis de las garantías derivadas del principio de legalidad penal -ya sea desde una perspectiva debilitada internacional o desde la concepción clásica del Derecho español o continental[405]- en la actualidad el mismo introduce una serie de cuestiones de obligada observancia. A la clásica garantía criminal (la relativa a qué debe ser considerado como un acto delictivo, que es la más importante para el estudio que estamos realizando) se deben sumar la garantía penal, la garantía

[400] GARCÍA-PABLOS DE MOLINA, A.: *Introducción al Derecho Penal*, Ed. Universitaria Ramón Areces, 4º edición, Madrid, 2006, pp. 475 y ss.

[401] Se refiere a la relación entre el principio de legalidad y la legislación penal en materia de delitos informáticos MATA y MARTÍN, R. M.: *Delincuencia informática y derecho penal*, Ed. Edisofer, 1ª edición, Madrid, 2001, p. 12. También en el ámbito de la técnica legislativa, el principio de legalidad y la delincuencia informática ROMEO CASABONA, C. M: "De los delitos…" ob. cit. p. 14.

[402] HUERTA TOCILDO, S.: "Principio…" ob. cit. p. 16, formula conjuntamente principio y garantías como *nullum crimen nulla poena sine praevia lege scripta, stricta e certa.* La misma autora en HUERTA TOCILDO, S.: "El contenido…" ob. cit. p. 514.

[403] MUÑOZ CONDE, F. y GARCÍA ARÁN, M.: *Derecho*... ob. cit. p. 99. Además se encuentra recogido en la Declaración Universal de Derechos Humanos de 10 de diciembre de 1948, en el Convenio Europeo para protección de los Derechos Humanos y las Libertades Fundamentales de 4 de noviembre de 1950 y en el Pacto Internacional de Derechos Civiles y Políticos de Nueva York de 19 de diciembre de 1966.

[404] Esta situación se estudia en HUERTA TOCILDO, S.: "El contenido…" ob. cit. pp. 541, donde se concluye que "el contenido del principio de legalidad reconocido en el artículo 7 del Convenio [de Roma] no coincide con el tradicionalmente atribuido a dicho principio, desde sus mismos orígenes, en los ordenamientos jurídicos de corte continental […] La peculiar versión del principio de legalidad contenida en el artículo 7 del Convenio constituye un *standard* mínimo de exigencias".

[405] Para la primera perspectiva véase HUERTA TOCILDO, S.: "El contenido…" ob. cit. Para la segunda HUERTA TOCILDO, S.: "Principio…" ob. cit. o más recientemente HUERTA TOCILDO, S.: "Artículo 25.1. El Derecho a la legalidad penal" en *Comentarios a la Constitución Española en su XXX Aniversario*, Ed. Wolters Kluwert, 1ª edición, Madrid, 2009.

procesal y la garantía de ejecución, operando en todas ellas el principio de legalidad penal[406]. Pero como acabamos de señalar, el ámbito que ahora nos interesa es el derivado de la garantía criminal, aquel que se refiere al momento de la definición legal de las conductas típicas[407]. Es aquí donde reside de forma más intensa la necesidad de una buena técnica legislativa, pues a la hora de definir qué acciones pueden ser constitutivas de delito -y qué penas llevan aparejadas (garantía penal)- resulta especialmente necesaria una buena construcción de las leyes[408]. La correcta redacción de las conductas punibles es una cuestión fundamental para conseguir la seguridad jurídica que se establece en la Constitución.

El principio de legalidad en materia penal además se manifiesta en otra serie de requisitos impuestos al legislador a la hora de aplicar el *ius puniendi* del Estado. Hablamos en concreto de la reserva de ley orgánica en materia penal, del mandato de taxatividad, de la prohibición de retroactividad o exigencia de ley previa, la prohibición de la analogía y el principio *de non bis in idem*[409]. Son especialmente importantes para nuestro estudio el mandato de taxatividad y la garantía de seguridad jurídica, por ser los que directamente afectan a la técnica legislativa. Así, para que la ley pueda cumplir con la función que le ha sido atribuida, esto es, señalar cuáles deben ser las conductas punibles, ésta debe ser clara y concisa, evitando la aparición de una terminología ambigua, con varios posibles significados, o que dé lugar a una interpretación que pueda vaciar de contenido el precepto[410], cuestión que, como veremos en las próximas páginas, no ha sido siempre respetada en materia de delincuencia informática.

---

[406] HUERTA TOCILDO, S.: "Principio..." ob. cit. pp. 16 y ss.; MIR PUIG, S.: *Derecho…* ob. cit. pp. 106 y 107, o QUINTERO OLIVARES, G.: *Parte*… ob. cit. pp. 54 y ss.

[407] MUÑOZ CONDE, F. y GARCÍA ARÁN, M.: *Derecho*... ob. cit. p. 100.

[408] Señalaba el Magistrado-Juez VELASCO NÚÑEZ respecto a la delincuencia informática (aunque es extensible a cualquier reforma legislativa), que "las reformas deben pensarse. Tienen que tener un sentido general y estructural", en relación con que la tipificación de conductas delictivas relativas a la informática debe tratarse en su conjunto, como una estructura, y no diversificar en exceso las mismas, sino concentrar sus puntos comunes (que son muchos) en la tipificación final que realiza el legislador. (Entrevista realizada por http://www.diariojuridico.com al Magistrado-Juez Don Eloy VELASCO NÚÑEZ en fecha 4 de noviembre de 2012).

[409] HUERTA TOCILDO, S.: "Principio…" ob. cit. pp. 18 y ss. o ZUGALDÍA ESPINAR, J. M.: *Fundamentos de derecho penal*, Ed. Tirant lo Blanch, 4ª edición, Valencia, 2010, pp. 111 y ss.

[410] Por todos, MUÑOZ CONDE, F. y GARCÍA ARÁN, M.: *Derecho*... ob. cit. p. 105.

Es decir, el precepto penal que se construye debe poder ser observado con certeza sobre su significado, y no dar lugar a dudas de lo que pretende, siendo esta cuestión de vital importancia al hablar de técnica legislativa en materia penal[411]. Por ello el legislador a la hora de redactar los tipos penales debe huir de la idea de introducir términos excesivamente amplios o vagos, que permitan diferentes interpretaciones de los mismos preceptos, así como de hacer mención a conceptos indeterminados. Baste ahora señalar que uno de los problemas principales de la legislación penal en materia de daños informáticos radica en que se ha decidido utilizar largas listas de acciones, así como la introducción de elementos de interpretación polisémica y otros conceptos indeterminados, que lejos de contribuir a la seguridad jurídica se alejan de ella, en pos de conseguir una mayor protección general y evitar la exclusión de la tipicidad de acciones futuras que ahora no es capaz de prever. Aunque, es cierto también, que no siempre el legislador puede evitar introducir en la redacción de los tipos este tipo de problemas, e incluso, en ocasiones puede resultar adecuado. Para resolver las dudas que se puedan generar siempre existirá el tamiz interpretativo de los jueces y tribunales a la hora de aplicar el precepto al caso concreto[412], así como la posibilidad de acudir a la doctrina científica para completar el significado de cada concepto, pero aun afirmando este extremo, se debe evitar caer en la idea de que el operador (jurídico o científico) siempre estará ahí para interpretar el precepto; se deben, por tanto, proyectar los esfuerzos hacia la máxima concreción a la hora de la redacción legislativa de los preceptos[413]. Consecuencia directa de aplicar de forma correcta este principio de taxatividad a la

[411] Así lo ha expresado el Tribunal Constitucional en la STC 62/1982, de 15 de octubre.

[412] En el sistema de fuentes del Derecho español, el art. 1.6 Código civil señala que "la jurisprudencia complementará el ordenamiento jurídico con la doctrina que, de modo reiterado, establezca el Tribunal Supremo al interpretar y aplicar la Ley, la costumbre y los principios generales del derecho". Sobre este extremo se puede consultar MESTRE DELGADO, J. F.: "Sobre el valor de la jurisprudencia en Derecho español" en *Revista General de Derecho Público Comparado*, nº 3, 2008.

[413] Cuando el legislador establece tipos manifiestamente abiertos de tal forma que con la lectura del precepto no se sabe bien en qué momento uno puede incurrir en la conducta típica, por ejemplo en tipos penales que afectan a ciertos objetos materiales como pueden ser el orden público o los intereses generales (en ningún lugar se define lo que son) o preceptos que contienen referencias a resultados graves como el caso de los daños informáticos (en los que no se introduce ningún método valorativo de cuándo un resultado se debe considerar grave), o preceptos que incluyen pluralidad de acciones, medios o resultados indeterminados (cuando se utiliza la fórmula "cualquier otro" o similares), también presentes en los delitos estudiados en esta investigación; se produce una excesiva dependencia del intérprete de la ley.

hora de definir los preceptos penales es la consiguiente aparición de la llamada seguridad jurídica en el ordenamiento, que representa la seguridad de que se conoce, o se puede conocer, lo previsto como prohibido, mandado o permitido por el poder público, en este caso por el legislador penal.

Sin embargo, junto a la existencia de los principios constitucionales enunciados, encontramos la realidad legislativa, en la que aparece la llamada legislación motorizada; y aunque no es el único de los problemas que acechan a la legislación emanada de las Cortes Generales[414], es quizá uno de los más importantes. Especialmente porque a partir de esta forma de legislar se producen con mayor o menor medida otras consecuencias igualmente nefastas para el ordenamiento jurídico en su conjunto, que siempre van a suponer una merma de la seguridad jurídica tan necesaria a la que hacíamos referencia. Esta idea relativa al método de elaboración de las leyes (la "legislación motorizada") ha sido tratada por diversos autores, pero también reconocida en la propia jurisprudencia de nuestro Tribunal Supremo, que ha acuñado esta misma expresión[415]. Autores en general críticos con la técnica legislativa actual, que de forma muy aproximada y general establecen la inoperancia o insuficiencia de la conexión entre la realidad necesitada de regulación, la política y el Derecho[416]. En general, suele entenderse por legislación motorizada la situación creada a partir de la relación que existe entre la velocidad de aprobación e inserción de normas en el ordenamiento y su posterior modificación o derogación en breves espacios de tiempo[417] al referirse a asuntos que en una sociedad compleja necesitan

[414] Véase VANDELLI, L.: *Trastornos de las instituciones políticas*, Ed. Trotta, 1ª edición, Madrid, 2007.

[415] Sentencia de TS, Sala 3ª, de lo Contencioso-Administrativo, 2 de Noviembre de 1987.

[416] En el ámbito de nuestra investigación se refieren a ello CONSENTINO, G.; GARCÍA, J. A.; TEJERO, D. O. y TEJERO N. F.: "Tras los pasos de la Seguridad perdida. Delitos informáticos" en *Informática y derecho. Revista iberoamericana de derecho informático*, nº 23, 24, 25 y 26, 1998, p. 1212 al señalar que a la hora de legislar "se suma […] la falta de especialización en el tema en análisis de quienes deben dar respuestas a la necesidad de tutelar los bienes jurídicos que se afectan por esta nueva forma de delinquir".

[417] Se refieren a ella entre otros muchos, GARCÍA DE ENTERRÍA, E. y FERNÁNDEZ RODRÍGUEZ, T.R.: *Curso de Derecho administrativo. Tomo I*, Ed. Civitas, 15ª edición, Madrid, 2011, p. 75, "el legalismo desenfrenado, volcado a una inestabilidad permanente". También GARCÍA DE ENTERRÍA, E: *Justicia y Seguridad Jurídica en un Mundo de Leyes Desbocadas*, Ed. Civitas, 1ª edición Madrid, 1999 (reimpresión de 2006). Y otros como GONZÁLEZ ORDOVÁS, M. J.: *Ineficacia, anomia y fuentes del derecho*, Ed. Dykinson, 1ª edición, Madrid, 2003; BUSTOS PUECHE, J. E.: "Incontinencia

de rápida adaptación legislativa. Un ejemplo de ello se manifiesta con la situación de la Decisión Marco que regula los daños informáticos que, previsiblemente, va a ser sustituida en un corto espacio de tiempo, lo que conllevará nuevamente la reforma del Derecho español en la materia. Y todo ello sin olvidar que tanto la Constitución Española, como los principios rectores del funcionamiento de la Unión exigen una serie de principios garantes de los Derechos básicos de los ciudadanos que, a pesar de todos los problemas que puedan aparecer, deben ser respetados.

Pero es que además, respecto de los delitos informáticos y de los daños informáticos, la necesidad de una rápida adaptación a la normativa internacional se ha manifestado, habitualmente, en dos velocidades. Por un lado -como ya hemos señalado- el legislador español llegó prácticamente con una década de retraso al desarrollo legislativo penal en este ámbito, lo que podría inducir a pensar que contó con el suficiente tiempo para realizar la correcta formulación de tipos penales (casi una década en la primera introducción de daños informáticos en 1995, y más de un lustro en la profunda reforma de éstos en 2010) acordes a las recomendaciones internacionales y formando un núcleo fácilmente reconocible en nuestro Derecho penal como así parece desprenderse de la normativa internacional. Sin embargo esto no ha ocurrido así; la segunda velocidad del proceso legislativo en materia de daños informáticos en España se ha caracterizado siempre por la inclusión de las reformas de este ámbito junto a modificaciones estructurales de nuestro ordenamiento penal (Código de 1995 y reforma sustancial de 2010), en cuyo proceso el legislador no se ha detenido especialmente en la concepción de la delincuencia informática como algo más que tipos prácticamente residuales de otros delitos preexistentes y tradicionales en nuestro ordenamiento. En resumen, mientras que el legislador ha tardado en acometer las reformas necesarias en este ámbito, cuando lo ha hecho, al verse rodeado de otros cambios del ordenamiento penal que presumiblemente se consideraban de mayor trascendencia, no se ha producido un estudio detenido sobre

---

legislativa, pobreza de resultados" en *Anuario de la Facultad de Derecho de Alcalá de Henares*, s/n, 2006, pp. 230-235; GARRIDO MAYOL, V.: *Las garantías...* ob. cit. pp. 17 y ss. o GARCÍA-ESCUDERO MÁRQUEZ, P.: "Nociones de técnica legislativa para uso parlamentario" en *Revista Parlamentaria de la Asamblea de Madrid*, nº 13, 2005, pp. 121 y ss.

el fenómeno en cuestión[418]. Comprobaremos a qué nos estamos refiriendo cuando se estudie el proceso de elaboración de la actual formulación de los tipos penales del artículo 264 CP, en la que tanto en sede del Ministerio como en sede parlamentaria se tramitó la propuesta prácticamente sin discusión alguna.

A pesar de todo ello, y aunque dedicaremos la tercera parte de la investigación al planteamiento de nuevos puntos de vista respecto de la delincuencia y los daños informáticos, no podemos negar que la actual regulación cumple aceptablemente bien las exigencias constitucionales respecto de la ley penal. Parece difícil pensar que el Tribunal Constitucional deba manifestarse en este ámbito. Los posibles problemas que pueda padecer la regulación de los daños informáticos siempre van a poder ser resueltos por la vía de la interpretación realizada por doctrina y jurisprudencia, si bien como manifestaremos llegado el momento, ello no obsta para realizar una propuesta de cambio sustancial que mejore aquellos puntos que puedan generar dudas en torno a los delitos de daños informáticos.

b.2. La reforma de los daños informáticos del artículo 264 CP.

El origen de la regulación actual de los daños informáticos del artículo 264 CP se encuentra en los trabajos de la Comisión General de Codificación llevados a cabos en una Sección especial entre los años 2005 y 2006[419], en los que se trató, además de la reforma de estos delitos, una revisión considerable del Código penal vigente. En primer lugar, debemos señalar que si bien los Estatutos se refieren a la existencia de cinco secciones permanentes en la Comisión General de Codificación, donde la cuarta es la designada para los trabajos en materia penal; en la actualidad, la Sección cuarta dedicada al Derecho penal no se encuentra en funcionamiento, es

[418] En la tercera parte de esta investigación nos detendremos en estos aspectos. Por ahora, entre muchos otros, se manifiesta MATA y MARTÍN, R. M.: "Criminalidad informática: una introducción al cibercrimen" en *Actualidad penal*, nº 36, 2003, pp. 936, al señalar que "el legislador penal, antes de tomar decisiones apresuradas en este campo deberá contar con estudios e informes previos de personas e instituciones especializadas en su análisis".

[419] DÍEZ RIPOLLÉS, J. L.: *La racionalidad…* ob. cit. p. 43, "esta etapa prelegislativa burocrática se ha convertido en la práctica en el momento determinante de las decisiones legislativas, en detrimento de la fase legislativa, la única formalmente competente para tomar la decisión".

más, desde la aprobación de los Estatutos en 1997[420] nunca se ha puesto en funcionamiento. Lo que no quiere decir, como ya hemos expresado, que no se hayan realizado trabajos en la materia.

Toda modificación penal que se lleve a cabo por iniciativa del Gobierno debe pasar por una fase prelegislativa gubernamental. En ella quedan vinculada la voluntad política de reforma, y en su caso las aportaciones científicas o de los grupos de presión expertos. Vistos los antecedentes en nuestra tradición penalista, se ha tratado siempre de una fase en la que en el seno de diferentes órganos del Ministerio de Justicia -a veces la Comisión General de Codificación, pero en otras ocasiones otros Departamentos del Ministerio- se ha reunido a los más prestigiosos penalistas (catedráticos, magistrados, etc.), generalmente sin la participación de profesionales de otros campos[421]. En nuestro caso debemos centrarnos en el concreto proceso de elaboración cuando los trabajos prelegislativos se realizan en la Comisión General de Codificación[422], sede de la propuesta de reforma del artículo 264 del Código penal.

En el caso de estos trabajos del periodo 2005-2006 no se llevaron a cabo en la Sección cuarta de la Comisión, que se encuentra inactiva; sino que se creó una Sección especial. Al amparo del artículo 22 de los Estatutos se constituyó por Orden de 8 de abril de 2005, en el seno de la Comisión General de Codificación, una Sección Especial para la Revisión del Código Penal[423]. En estos trabajos de

[420] Real Decreto 160/1997, de 7 de febrero, por el que se aprueban los Estatutos de la Comisión General de Codificación.

[421] DÍEZ RIPOLLÉS, J. L.: *La racionalidad…* ob. cit. p. 49. Desde una perspectiva compartida en esta investigación, ALAMILLO DOMINGO, I.: "Las políticas…" ob. cit. p. 13, manifiesta que "se considera que los gobiernos, por sí solos, no pueden gestionar todos los retos y cuestiones de seguridad [informática], lo que implica una necesidad de involucrar al sector privado y a la sociedad civil, efecto que se puede conseguir con diferentes instrumentos, como las asociaciones público-privadas, el desarrollo de mejores prácticas, el suministro de consejo y la participación en órganos comunes".

[422] Para un estudio aproximado del funcionamiento de la Comisión General de Codificación y su papel en esta reforma penal véase GONZÁLEZ HURTADO, J. A.: *Aproximación a la fase prelegislativa en la elaboración de normas penales. La Comisión General de Codificación y el Derecho penal en la actualidad*, Ed. Dykinson, 1ª edición, Madrid, 2013, pp. 51 y ss.

[423] Memoria de la Comisión General de Codificación de 2005. Señala además que "se encomienda a la Sección Especial una revisión del vigente Código Penal con motivo de los diez años transcurridos desde su aprobación. La Sección elaborará una propuesta de Anteproyecto de ley orgánica de reforma del Código Penal que, junto con su Exposición de motivos y Memoria justificativa, elevará al Ministro

modificación parcial del Código penal, la participación de expertos de prestigio en la sede de la Comisión ha sido reducida, siendo generalmente sesiones de entre ocho y diez miembros, que tuvieron la responsabilidad de formular las propuestas de modificación solicitadas en las diferentes partes del Código penal afectadas[424]. Dicha Sección mantuvo 19 reuniones entre el 8 de abril de 2005 y el 27 de junio de 2006. Aunque la Sección especial tuvo su primera reunión el 5 de abril de 2005, no es hasta la sesión del día 31 de mayo cuando comienzan los trabajos para modificar el Código penal[425] en la cual se entregó el anexo en el que constaban las diferentes materias contenidas en el Código penal sobre las que se proponía una revisión; señalando además el acuerdo para solicitar informes a diferentes instituciones y organismos del Estado para "que pongan de manifiesto la necesidad concreta de reformas penales". Tras ello fueron asignadas las ponencias a los diferentes componentes de la Sección, siendo normalmente trabajos en diferentes extremos jurídicos los llevados a cabo por cada vocal[426].

---

de Justicia. La Sección Especial se configura como un órgano colegiado de asesoramiento en la preparación de las tareas prelegislativas del Ministerio de Justicia, conforme a lo previsto en los Estatutos de la Comisión General de Codificación. En el desarrollo de sus trabajos se atenderá a las directrices generales de política legislativa que indique el Ministro de Justicia".

[424] La reciente reforma del Código penal, aprobada en 2010, que modificaba más de 150 artículos, tanto de parte general como de parte especial, fue enteramente desarrollada por la Sección especial presidida por D. José Jiménez Villarejo, Ex-Presidente de la Sala II del Tribunal Supremo, integrada por los Vocales: D. Luis Arroyo Zapatero, Catedrático de Derecho Penal; D. Juan Carlos Carbonell Mateu, Catedrático de Derecho Penal; D. Pedro Crespo Barquero, Fiscal Secretaría Técnica de la Fiscalía General del Estado; D. Carlos García Valdés, Catedrático de Derecho Penal; D. José Luis González Cussac, Catedrático de Derecho Penal; D. Francisco Muñoz Conde, Catedrático de Derecho Penal; D. Gonzalo Quintero Olivares, Catedrático de Derecho Penal; Dª Isabel Valldecabres Ortiz, Asesora del Gabinete del Ministro de Justicia y D. Luis P. Villameriel Presencio, Secretario General Técnico del Ministerio de Justicia; interviene como Vocal Secretario D. Rafael Alcalá Pérez-Flores, Magistrado. [Memoria de la Comisión General de Codificación del año 2006].

[425] La sesiones de 5 y 19 de abril, y 10 de mayo de 2005 tuvieron como objeto los trabajos para la modificación de la Ley Orgánica 5/2000, de 12 de enero, reguladora de la responsabilidad penal de los menores.

[426] El número de vocales nombrados para la Sección especial fue muy inferior al de artículos y contenidos de los que cursar propuesta de reforma. No sería lógico asignar un ponente por artículo, pero tampoco parece un procedimiento eficaz asignar a cada uno de los pocos vocales la elaboración de los trabajos de reforma de un considerable número de artículos, cuando además estos ponentes no se dedican de forma exclusiva a los trabajos de estudio durante el periodo existencia de la Sección especial, sino que continúan todos ellos con sus labores profesionales.

Aunque en 2007 se realizó una reforma legislativa penal en materia de seguridad vial[427] que tiene su origen en estos trabajos de la Comisión, más importante, tanto para nuestro estudio como en general, es la que fue operada por la entrada en vigor de la LO 5/2010, de 22 de junio, en la que se modificaron más de 150 artículos, tanto de la parte general del como de la parte especial. Esta reforma introduce en el ordenamiento, con mayores o menores cambios tras el debate legislativo, prácticamente todas las propuestas realizadas en el seno de la Sección penal de la Comisión General de Codificación. Cabe destacar que estos trabajos de la Comisión ya fueron convertidos en proyecto de ley por el ejecutivo durante el año 2007[428], proyecto que no llegó a fructificar debido al final de la legislatura[429], y que fue presentado de nuevo al Congreso en la siguiente legislatura en el año 2009[430]. Proyecto que resultará el finalmente aprobado tras los trámites y modificaciones oportunos en las Cortes Generales.

Pero volviendo a nuestro ámbito de estudio, la reforma en materia penal de los llamados daños informáticos extrae su redacción del anteproyecto de ley elaborado en los trabajos de la Comisión General de Codificación del Ministerio de Justicia comenzados en el año 2005[431]. En ella se encomienda al ponente la propuesta de regulación en dicha materia, materia que a su vez proviene de la imposición europea a través de una Decisión Marco (Decisión Marco 2005/222/JAI relativa a los ataques a sistemas informáticos). De los documentos que se aportan en el seno de la Comisión General de Codificación no se puede apreciar, por desgracia, un debate sobre la conveniencia de la forma de regular dichos delitos de nuevo cuño.

---

[427] Véanse CARBONELL MATEU, J. C.: "La reforma del tratamiento penal de la seguridad vial" en MORILLAS CUEVA, L.: *Delincuencia en materia de tráfico y seguridad vial*, Ed. Dykinson, 1ª edición, Madrid, 2008 o ROSÓN FERNÁNDEZ, A.: "La reforma de los delitos contra la seguridad vial. La L.O. 15/2007" en *La Ley, edición electrónica*, Julio 2009.

[428] Boletín Oficial de las Cortes Generales. Congreso de los Diputados. Serie A, 15 de enero de 2007, núm. 119-1.

[429] El último trámite que fue llevado a cabo fue la aprobación de ampliación de plazo de enmiendas. Boletín Oficial de las Cortes Generales. Congreso de los Diputados. Serie A, 19 de diciembre de 2007, núm. 119-35.

[430] Calificación en el Boletín Oficial de las Cortes Generales. Congreso de los Diputados. Serie A, 27 de noviembre de 2009, núm. 52-1.

[431] Ministerio de Justicia, Comisión General de Codificación, Sección especial para la revisión del Código penal: Libro 2, sesiones del 06.07.05 al 20.12.05, pp.76-79; y Libro 4, sesiones del 28-3-06 AL 27-6-06 p. 12-13, 69-74 y 76-77

La propuesta realizada -no hay constancia de que haya llegado a ser debatida- es la que finalmente fue aprobada por la Sección, y con algunos cambios menores que analizaremos a continuación es la que se encuentra en vigor.

En los documentos de la Comisión tampoco es posible encontrar una motivación pormenorizada que explique la idoneidad de introducir dicha modificación de la forma efectivamente realizada. Este ejemplo es ilustrativo, pues precisamente en una materia como la de los delitos informáticos, con un fuerte contenido técnico, es importante no limitarse a transcribir la normativa europea sino hacer un verdadero ejercicio de transposición para el que en algunos casos parece hacerse inevitable el concurso de expertos en otras materias, por ejemplo en telecomunicaciones, como sería el caso que nos ocupa; participación que como ya señalamos en su momento, no se produce al menos, de forma oficial. Cabría preguntarse entonces si durante la redacción de la propuesta se han consultado otras fuentes, externas a la Comisión, para realizar de la forma en que lo ha hecho su redacción, cuestión que sería del todo lógica, aunque no conste en las actas de las reuniones mantenidas por el grupo de trabajo. Consultas externas que en una materia técnica son necesarias, y cuya ausencia pueden hacer preguntarnos sobre la pertinencia de establecer un mecanismo reglado de consultas a profesionales externos, cuyas consideraciones consten finalmente también en las actas de las reuniones; redundando así en la publicidad y transparencia de las decisiones prelegislativas, pero sobretodo en la calidad final de las propuestas. Posibilidad que si bien los Estatutos recogen en el artículo 20.4 designando al Ministro de Justicia como el competente para autorizarlas, no parece el procedimiento más adecuado y ágil.

C) TEXTO DE LA COMISIÓN GENERAL DE CODIFICACIÓN, DEL PROYECTO DE LEY Y DE LA LO 5/2010 DE 22 DE JUNIO.

El texto resultado de la propuesta de la Comisión General de Codificación del artículo 264 CP quedó redactado de la siguiente manera:

> *1. El que sin autorización y de manera grave borrase, dañase, deteriorase, alterase, suprimiese, o hiciese inaccesibles datos, o programas ajenos, será castigado, en*

consideración a la gravedad del hecho, con la pena de prisión de seis meses a dos años.

2. El que sin estar autorizado y de manera grave obstaculizara o interrumpiera el funcionamiento de un sistema de información, introduciendo, transmitiendo, dañando, borrando, deteriorando, alterando, suprimiendo o haciendo inaccesibles datos informáticos, será castigado, atendiendo a la gravedad del hecho, con la pena de prisión de seis meses a tres años.

3. Se impondrán las penas superiores en grado a las respectivamente señaladas en los dos apartados anteriores y, en todo caso, la pena de multa del tanto al décuplo del perjuicio ocasionado, cuando en las conductas descritas concurra alguna de las siguientes circunstancias:

- Se hubiese cometido en el marco de una organización criminal.

- Haya ocasionado daños de especial gravedad o afectado a los intereses generales.

Entre la propuesta elaborada por la Comisión General de Codificación y la finalmente planteada en el Proyecto de Ley encontramos algunos cambios que conviene al menos señalar:

*1. El que **por cualquier medio**, sin autorización y de manera grave borrase, dañase, deteriorase, alterase, suprimiese, o hiciese inaccesibles datos o programas informáticos ajenos, **cuando el resultado producido fuera grave**, será castigado con la pena de prisión de seis meses a dos años.*

*2. El que **por cualquier medio**, sin estar autorizado y de manera grave obstaculizara o interrumpiera el funcionamiento de un sistema **informático ajeno**, introduciendo, transmitiendo, dañando, borrando, deteriorando, alterando, suprimiendo o haciendo inaccesibles datos informáticos, **cuando el resultado producido fuera grave**, será castigado, con la pena de prisión de seis meses a tres años.*

3. Se impondrán las penas superiores en grado a las respectivamente señaladas en los dos apartados anteriores y, en todo caso, la pena de multa del tanto al décuplo del perjuicio ocasionado, cuando en las conductas descritas concurra alguna de las siguientes circunstancias:

- Se hubiese cometido en el marco de una organización criminal.

- Haya ocasionado daños de especial gravedad o afectado a los intereses generales.

4. Cuando de acuerdo con lo establecido en el artículo 31 bis una persona jurídica sea responsable de los delitos comprendidos en este artículo, se le impondrán las siguientes penas:

- Multa del doble al cuádruple del perjuicio causado, si el delito cometido por la persona física tiene prevista una pena de prisión de más de dos años.

- Multa del doble al triple del perjuicio causado, en el resto de los casos.

Atendidas las reglas establecidas en el artículo 66 bis, los jueces y tribunales podrán asimismo imponer las penas recogidas en las letras b a g del apartado 7 del artículo 33.

En la transcripción anterior hemos señalado las variaciones entre el texto de la Comisión y el finalmente incluido en el proyecto aunque, como veremos, se trata de cambios de importancia relativa en cuanto al contenido de los delitos de daños informáticos. Podemos observar, en primer lugar, que el proyecto final ha decidido aclarar la forma de comisión de los delitos de daños informáticos al añadir la fórmula "por cualquier medio" que no constaba en los trabajos prelegislativos de la Comisión. Se trata de un cambio que trata de clarificar la forma de cometer las acciones típicas, si bien no introduce novedades excesivas por cuanto, al no señalarse los medios, la idea general sería entender, si el legislador no lo ha introducido, que es válido cualesquiera. En todo caso siempre es de agradecer la aclaración añadida, que elimina de una interpretación lógica la idea de que los daños informáticos sólo puedan ser cometidos por manipulaciones informáticas. También en ambos tipos penales de daño se sustituye la expresión "en consideración a la gravedad del hecho" por la más concreta de "cuando el resultado producido fuera grave". Aunque nos detendremos sobre esto al analizar el tipo objetivo, cabe señalar que el cambio sí modifica aspectos del contenido de los delitos, ya que la literalidad de la opción de la Comisión introducía algunas dudas: por un lado sobre si toda acción quedaría tipificada, y la consideración de dicha gravedad sólo incidiría en la determinación concreta de la pena, lo que ha quedado resuelto con la siguiente (y a la postre definitiva) redacción en la que se manifiesta que sólo será típica la acción cuyo resultado se repute grave; por otro lado, el texto de la Comisión puede generar dudas en cuanto a si la gravedad debe ser en las acciones o en el resultado pues usa la expresión "gravedad de los hechos", hechos que ya presentan un elemento de

gravedad en el texto de la proposición; lo que supone un nuevo elemento generador de dudas, y cuyo cambio se debe aplaudir.

También se sustituye en el artículo 264.2 CP el objeto del delito, que pasa de ser los "sistemas de información "a los "sistemas informáticos", cambio menor, que no reviste especial consideración, pero se aleja de la Decisión Marco de 2005. Así como la introducción de la ajenidad del mismo, que sí constaba en el delito del apartado primero, pero no así en el del apartado segundo del artículo 264 CP. Además de las diferencias anteriores, los trabajos de la Comisión no reflejan los aspectos de punibilidad sobre las personas jurídicas cuando éstas cometen los delitos, aunque podemos señalar que la forma final de regulación propuesta y aprobada no supone novedad alguna al método habitual seguido por el legislador para introducir la responsabilidad penal de las personas jurídicos en el resto de tipos del Código.

Por todo ello, si algo queda de manifiesto, y lo confirmaremos a continuación, es que la labor más intensa en la elaboración de la actual regulación de daños informáticos ha tenido lugar en esta fase prelegislativa y no en la tramitación en las Cortes Generales, como podría presumirse erróneamente. Por lo demás, el anteproyecto de normativa penal que nos ocupa sigue el trámite general para su final conversión en proyecto de ley que será presentado en las Cortes Generales para la tramitación parlamentaria[432].

[432] GARCÍA-ESCUDERO MÁRQUEZ, P.: "Consideraciones…" ob. cit. pp. 34 y 35, en primer lugar, el anteproyecto ha de ser objeto de examen por la Comisión de Secretarios de Estado y Subsecretarios que prepara la reunión del Consejo de Ministros. En esta reunión se realizará una primera deliberación respecto a la idoneidad, contenido y momento de elevar el mismo al Consejo. Como resultado de dichas deliberaciones, el anteproyecto puede ser incluido en el orden del día del Consejo de Ministros. En ese caso, a su vez puede incluirse dentro de las cuestiones informadas favorablemente o no, lo que no desecha la posibilidad de conversión del anteproyecto, sino que remite a un estudio más detenido del propio Consejo de Ministros. Normalmente los anteproyectos de ley, especialmente cuando se trata de materias muy relevantes como puede ser el caso de la legislación penal, siempre son debatidos por el Consejo de Ministros, incluso a pesar haber sido informados favorablemente. La Ley del Gobierno establece que la aprobación del anteproyecto de ley junto con sus informes en proyecto de ley debe realizarse a través de un Acuerdo del Consejo de Ministros (Art. 25.d LG: "Acuerdos del Consejo de Ministros, las decisiones de dicho órgano colegiado que no deban adoptar la forma de Real Decreto"). Será en la reunión del Consejo de Ministros cuando se decidirá finalmente su aprobación, o la necesidad de añadir nuevos informes o consultas amen de aquellas que hemos señalado como preceptivos (Art. 22.3 LG: "El titular del Departamento proponente elevará el Anteproyecto al Consejo de Ministros a fin de que éste decida sobre los ulteriores trámites y, en particular, sobre las consultas, dictámenes e informes que resulten convenientes, así como sobre los

Finalmente, en la fase legislativa -la parte más importante para la aprobación de leyes, o al menos así debe considerarse desde un punto de vista procedimental[433]- en cuanto al interés de ésta en nuestro estudio es mínimo. En efecto la regulación de los daños informáticos vigente en nuestro ordenamiento penal pasó por la tramitación legislativa casi desapercibida. Ya señalamos que la reforma de los delitos de daños informáticos se produjo en una ley general de reforma del Código penal, por lo que los aspectos tratados tanto en fase prelegislativa y legislativa fueron de una cantidad considerable. Pues bien, en la tramitación parlamentaria, los procedimientos en las Cortes (Congreso de los Diputados y Senado), la propuesta del proyecto de ley del Gobierno pasó casi inalterada. La única variación que se produjo fue la introducción de los "documentos electrónicos" como objeto del delito en el 264.1 CP, siguiendo la tripartición de objetos del delito contenida en la regulación anterior y que no despierta consideraciones importantes ya que, en todo caso, la desaparición de este elemento no supondría un problema de entidad, al poder englobarse perfectamente los documentos electrónicos como un tipo de datos informáticos.

Por lo demás, el texto del proyecto y el finalmente aprobado es exacto punto por punto al del proyecto de ley. De los diarios de las Cortes respecto de la tramitación parlamentaria en la Comisión de Justicia del Congreso, posteriormente en el Pleno y finalmente en el Senado se extrae que en meses de planteamiento y defensa de enmiendas a otros aspectos de la reforma del Código penal, sólo fueron

términos de su realización, sin perjuicio de los legalmente preceptivos"). En caso de acordarse nuevos informes, la aprobación se verá suspendida hasta que éstos sean presentados, procediendo de nuevo a debatirse en un Consejo de Ministros posterior, para en caso de su aprobación remitirse al Congreso de los Diputados junto con la exposición de motivos y la memoria y los demás informes y antecedentes necesarios para pronunciarse sobre él. Cabe señalar, que la aprobación del anteproyecto de ley por el Acuerdo del Consejo de Ministros, como acción del Gobierno, está sometido a un doble control, por un lado el control político a través del Congreso de los Diputados y el Senado; y por otro a través de la vía jurisdiccional competiéndole a los tribunales de lo contencioso-administrativos conocer de las impugnaciones de dichos acuerdos (Art. 26 LG: "1. El Gobierno está sujeto a la Constitución y al resto del ordenamiento jurídico en toda su actuación. 2. Todos los actos y omisiones del Gobierno están sometidos al control político de las Cortes Generales. 3. Los actos del Gobierno y de los órganos y autoridades regulados en la presente Ley son impugnables ante la jurisdicción contencioso-administrativa, de conformidad con lo dispuesto en su Ley reguladora. 4. La actuación del Gobierno es impugnable ante el Tribunal Constitucional en los términos de la Ley Orgánica reguladora del mismo").

[433] Art. 66.2 CE: "Las Cortes Generales ejercen la potestad legislativa del Estado, aprueban sus Presupuestos, controlan la acción del Gobierno y tienen las demás competencias que les atribuya la Constitución.".

planteadas tres enmiendas a este artículo, dos de ellas con objeto de modificar aspectos sobre la responsabilidad de las personas jurídicas (en función o no de la posibilidad de imputar a éstas penalmente acorde a la reforma del Libro I[434]), además de la ya mencionada introducción en el apartado primero del artículo 264 CP como objeto del delito de los documentos electrónicos, así como aumentar la penalidad del primer párrafo y establecer prisión de 1 a 3 años[435], siendo finalmente aceptada sólo la parte referente la inclusión de los documentos electrónicos como objeto del delito del artículo 264.1 CP.

3. ANÁLISIS DEL TIPO OBJETIVO

Una vez hemos introducido previamente la regulación actualmente en vigor, nos corresponde ahora abordar aquellos extremos referidos al tipo objetivo de las dos conductas descritas en el artículo 264 CP después de la entrada en vigor de la LO 5/2010 de 22 de junio, de reforma del Código penal.

En este apartado se pretende analizar la acción o acciones típicas del delito, investigando cuales son los elementos que dan lugar a su aparición, así como las distintas posibilidades de concurrencia de los elementos del injusto y el grado de ejecución. El análisis del bien jurídico protegido suscitará algunas cuestiones que se atenderán a continuación[436], así como todo lo relacionado con los sujetos intervinientes y el objeto material. En todo caso, y aunque en ocasiones serán

[434] Debemos recordar que en la legislación penal española no existía hasta la aprobación de la LO 5/2010, de reforma del Código penal, la responsabilidad penal de las personas jurídicas, lo que explica que según iban sucediéndose etapas en la tramitación de la ley, en función o no de la introducción o exclusión de la figura, se tratase de sancionar, aunque fuera civilmente, la responsabilidad de éstas en la comisión de estos delitos.

[435] La enmienda 355 presentada por el Grupo Parlamentario Popular en el Congreso justifica tales modificaciones del proyecto por cuanto en "la tipificación de los daños causados a datos informáticos, debería mantenerse la referencia actual en el 264.2 a "documentos electrónicos". Pensemos, por ejemplo, en un documento "scaneado" en un formato tif o pdf. Sólo con cierta dificultad podría considerarse el mismo como "dato informático" y, desde luego no es un programa que son las dos posibilidades que quedarían tras esta reforma. De forma que la conducta podría quedar impune y, sin embargo, parece claro que el daño al mismo debe también protegerse. Tampoco se encuentra justificación a rebajar la pena con carácter general desde 1 a 3 años que es la pena actual a de seis meses a dos años, cuando este tipo de delitos cada vez cobra más auge".

[436] Y que serán objeto de un profundo análisis en la tercera parte de la investigación al tratar algunas dudas que plantea la actual normativa, así como al tratar de elaborar una propuesta de regulación adecuada.

tratados de forma introductoria, el objetivo es ahora limitar el estudio a la situación actual de los delitos de daños informáticos, dejando el análisis de propuestas o problemas que se presentan en la actual regulación para el capítulo siguiente.

A) BIEN JURÍDICO PROTEGIDO EN LOS DAÑOS INFORMÁTICOS

La cuestión relativa al bien jurídico protegido plantea uno de los problemas que más dudas suscitan en los delitos de daños en general, y en los delitos de daños informáticos en particular.

A este respecto la doctrina parece dividirse en dos grupos, por una parte aquellos partidarios de entender que no existe un bien jurídico común en los delitos informáticos (no sólo los de daños, también incluiríamos aquí el conjuntamente modificado en el año 2010, artículo 197.3 del CP, ubicado en los delitos contra la intimidad, así como cualquiera de los otros que señalamos en la primera parte de la investigación[437]), por lo que cada tipo penal con relevancia en el campo de la informática que se pueda regular en el Código penal deberá estar ubicado en el Capítulo correspondiente al bien jurídico que se pretenda proteger[438]: así, por ejemplo, los delitos de daños informáticos, en el Capítulo dedicado a los daños, el delito de acceso ilícito a sistemas, junto con los delitos que protegen la intimidad, etc. Por otro lado, se ha venido desarrollando una nueva teoría acerca de si todos estos delitos, que giran en torno a la utilización o ataque a sistemas informáticos, pueden agruparse bajo un mismo bien jurídico común que trate de proteger, además de aquellos bienes específicos por razón de materia, un bien común[439].

---

[437] Por citar algunos, de la ya de por sí poco definida lista: robo con fuerza (239 CP) en relación con la utilización de llaves falsas (238.4 CP), la estafa informática (248.2.a CP), defraudaciones de fluido eléctrico (255 CP), delitos contra la propiedad intelectual (270.1 CP), delitos contra los servicios de radiodifusión e interactivos (286 CP), etc.

[438] ADÁN DEL RÍO, C.: "La persecución…" ob. cit. p. 156, señala que "es conocida, y quizá todavía aceptable, la posición de quienes sostienen que, en la mayor parte de los casos, la informática e Internet ha provocado diferentes modalidades delictivas por razón de los medios empleados o del lugar donde se desenvuelven, siendo estas modalidades un ataque más que se produce a los bienes jurídicos tradicionales. En este sentido, la no existencia de un título específico en nuestro Código Penal que acoja este tipo de delitos se considera un acierto del legislador de 1995".

[439] HUETE NOGUERAS, J.: "La reforma…" ob. cit. p. 1, plantea, sin profundizar en ella, una idea ecléctica en la que se puede observar tanto la diversificación de los tipos penales tradiciones, como la aparición de nuevos tipos que responden a la necesidad de proteger bienes jurídicos de nuevo cuño; reconociendo, en todo caso, que el legislador español ha optado por la idea primera.

Tal discusión no ha encontrado hasta el momento una resolución pacífica[440]. En principio, atendiendo a la sistemática del Código penal, parece apropiado, en el caso de los daños informáticos, entender que su bien jurídico objeto de protección es la propiedad ajena, tratándose por tanto de un bien jurídico individualizable sobre los sujetos titulares del patrimonio de que se trate[441]. De lo que no hay duda tampoco es que tal realidad se ha visto desbordada por la situación actual en la que parece difícil no aceptar que puedan existir otros bienes jurídicos amenazados por estas acciones delictivas[442].

La primera posición entiende que el bien jurídico en los tipos del artículo 264 CP es el patrimonio en particular y el orden socioeconómico en general, considerándose, por tanto, correcta la ubicación sistemática de los daños en el Capítulo en que actualmente se insertan. El bien jurídico a proteger no es sustancialmente diferente del que protege el artículo 263 CP referido a los daños clásicos, y la separación de unos y otros se debe a razones de mayor desvalor del resultado producido que comportan una necesidad de mayor penalidad, así como evitar las posibles lagunas en cuanto a los daños sobre elementos lógicos y no físicos[443], pero no a protecciones de diferentes de bienes jurídicos[444].

---

[440] Como señala RAGUÉS I VALLES, R. y ROBLES PLANAS, R.: "La reforma de los delitos informáticos: incriminación de los ataques a sistemas de información" en SILVA SÁNCHEZ, J. M. (dir.): *El nuevo código penal. Comentarios a la reforma*, Ed. La Ley, 1ª edición, Madrid, 2012, p. 373, "el principal problema al que se enfrenta el intérprete de esta figura delictiva es decantarse por un entendimiento fáctico-económico (interpretándola de forma próxima a los daños clásicos) o por un entendimiento ideal-funcional de estos daños (de forma relativamente autónoma a las figuras clásicas)".

[441] DE LA MATA BARRANCO, N. J.: "El delito…" ob. cit. p. 156.

[442] MARCHENA GÓMEZ, M.: "El sabotaje informático: entre los delitos de daños y los desórdenes públicos*"* en *Internet y Derecho penal. Consejo General del Poder Judicial*, número 10, Madrid, 2001, p. 363. También GALÁN MUÑOZ, A.: "Expansión e intensificación del derecho penal de las nuevas tecnologías: un análisis crítico de las últimas reformas legislativas en materia de criminalidad informática" en *Revista de Derecho y proceso penal*, nº 15, 2006, p. 30, al afirmar que "este planteamiento [ubicar los tipos referidos a la informática en las categorías clásicas] resulta erróneo, por cuanto en realidad estos nuevos tipos delictivos vendrían a proteger unos bienes jurídicos diferentes y, sobre todo, cualitativamente más amplios".

[443] MATA y MARTÍN, R. M.: "Criminalidad…" ob. cit. p. 80, concluye que la figura del antiguo 264.2 CP, (aplicable al actual 264 CP) viene a completar una posible laguna legal en cuanto a la inmaterialidad del objeto material, pero en ningún caso a tutelar nuevos bienes jurídicos.

[444] ORTS BERENGUER, E. y ROIG TORRES, M.: *Delitos informáticos y delitos cometidos a través de la informática* Ed. Tirant lo Blanch, 1ª edición, Valencia, 2001, pp. 81 y ss. También ROMEO

Sin embargo, como avanzamos, un nuevo sector doctrinal se inclina por pensar que la sistemática del Código penal no debe ser impedimento para encontrar en este tipo de delitos un bien jurídico algo diferente, relacionado siempre con el originario, pero que trasciende más allá del mismo y configura un nuevo bien digno de protección. Este sería, a grandes rasgos, la información y la accesibilidad a la información y la seguridad de los sistemas informáticos[445], luego se configuraría como un bien supraindividual y pluriofensivo, junto con el bien individualmente protegido.

Esta idea responde al hecho innegable de que la implantación de las nuevas tecnologías en nuestro entorno, tanto en las Administraciones Públicas como en las empresas privadas supone -a la vez que un avance en el nivel de vida de las personas- entregar a determinados sistemas informáticos un poder sobre el normal desarrollo de nuestras vidas de dimisiones colosales. No escapamos a la idea de que, efectivamente, los daños recogidos en el artículo 264 CP producen un perjuicio económico directo sobre ciertos sujetos, pero además de ello, el correcto funcionamiento de las nuevas tecnologías es un bien que los Estados deben proteger más allá de los perjuicios individuales que cada uno, en su esfera personal, pueda sufrir. Esta es la idea que se desprende especialmente del Convenio sobre la Ciberdelincuencia de Budapest de 2001 y la razón de existir del mismo y, puede pensarse, asimismo de la Decisión Marco 2005/222/JAI de 24 de febrero. Siguiendo esa progresión lineal, no debemos olvidar que la interpretación de la legislación

---

CASABONA, C. M.: "Delitos informáticos de carácter patrimonial" en *Informática y derecho. Revista iberoamericana de derecho informático*, nº 9, 10 y 11, 1996, p. 440, cuando señala que se inclina "por la vía de completar los tipos existentes allí donde resulte necesario […] sin necesidad de crear ningún tipo autónomo o específico". El mismo autor en ROMEO CASABONA, C. M: "De los delitos…" ob. cit. p. 15, al definir estos nuevos tipos penales como tipos de equivalencia entre el delito tradicional y su versión informática. Exactamente igual ROVIRA DEL CANTO, E.: *Delincuencia informática y fraudes informáticos*, Ed. Comares, Granada, 2002, p. 69 y 70, habla de creación de "tipos de equivalencia" que sirven para realizar una "interpretación correctiva, sistemática o correctora de los preceptos clásicos".

[445] Varios autores han pretendido, en torno a estas ideas, fijar un bien jurídico común, aunque sin demasiado éxito: ÁLVAREZ VIZCAYA, M.: "Consideraciones político criminales sobre la delincuencia informática: el papel del derecho penal en la red" en *Internet y Derecho penal. Consejo General del Poder Judicial*, número 10, 2001, p. 277, también RODRÍGUEZ MOURULLO, G., LASCURAIN SÁNCHEZ, J. A. y ALONSO GALLO, J.: *Derecho Penal e Internet* en FERNÁNDEZ ORDÓÑEZ, M. A., CREMADES GARCÍA, J. e ILLESCAS ORTIZ, R. (coords.): *Régimen Jurídico de Internet*, Ed. La Ley, 1ª edición, Madrid, 2001, p. 117.

estatal, en nuestro caso el Código penal, no debe obviar el origen del que toman partida sus tipos penales, y ese origen es el que ya hemos establecido. Visto de esta manera, no creemos que interpretar que existe un bien jurídico supraindividual distinto al propio de la protección por razón de ubicación en el Código choque contra una interpretación sistemática[446], por cuanto, el sistema penal, y más el ordenamiento jurídico en general, hoy en día, no se circunscribe sólo a las leyes nacionales, sino en gran medida a los Convenios y disposiciones internacionales ratificados por los Estados.

Como decimos, la situación actual en nuestro ordenamiento no tiene una respuesta clara, pues con los oportunos matices, ambos tipos de interpretaciones podrían subsistir. Se señala por la doctrina que estos problemas de ubicación y de unidad de protección de las conductas que nos ocupan pudieron deberse, en su momento, al interés de sancionar ciertas acciones que no se encontraban recogidas en nuestra regulación penal, si bien es cierto que no se atendió a un verdadero debate sobre el significado y alcance de las mismas, y las razones que justificaban su introducción[447]. Sea cual fuere la razón por la que en su momento se utilizase la fórmula elegida, no parece lógico que cerca ya de haber transcurrido dos décadas desde la regulación de estas conductas de daños informáticos nos encontremos todavía con que estas cuestiones no han sido oportunamente resueltas[448]. La prácticamente inexistente jurisprudencia al respecto y un escaso tratamiento doctrinal en profundidad han jugado además un papel importante en los motivos por los que no existe acuerdo. En todo caso, retomaremos esta cuestión en el capítulo cuarto de esta investigación, en el que será propuesto un marco sustancialmente diferente al

[446] MUÑOZ CONDE, F. y GARCÍA ARÁN, M.: *Derecho*… ob. cit. p. 126.

[447] La ubicación y sistemática seguida por el legislador de forma general en este Título XIII del Libro II -dejando al margen el problema concreto de nuestra investigación- ha sido criticada por la doctrina, así ZUGALDÍA ESPINAR, J. M.: "Los delitos contra la propiedad, el patrimonio y el orden socioeconómico en el nuevo Código Penal (consideraciones generales sobre el Título XIII del N.C.P)" en *Cuadernos de política criminal*, nº 59, 1996, pp. 417 y ss. Concretamente sobre los daños informáticos se refiere DE LA MATA BARRANCO, N. J.: "El delito…" ob. cit. pp. 160 y 161.

[448] ADÁN DEL RÍO, C.: "La persecución…" ob. cit. p. 156, ya señala, con acierto, que "no siendo partidaria en la mayor parte de los casos de lo que se viene denominando desbordamiento del ámbito penal o adelanto de la barrera de protección penal (según la posición que ocupa quien lo alega), ni de la extensión desmedida de los tipos penales, tengo la sensación, de que el problema crece y no se soluciona".

actual, en el que los problemas ahora expuestos quedarían importantemente reducidos y que acoge básicamente la segunda visión expuesta en este epígrafe.

B) ACCIÓN TÍPICA

Con la intención de seguir un método acorde con la estructura de la teoría jurídica del delito, comenzaremos señalando los elementos típicos que se integran en las dos figuras del nuevo artículo 264 CP. Tras ello, veremos qué modalidades de comisión pueden observarse en estos tipos en concreto ¿estamos ante delitos de acción, o son posibles las figuras de la omisión en los mismos? Finalmente se analizará el momento en que se sitúan las barreras de protección del bien jurídico para descubrir los posibles grados de ejecución en función de que estemos ante delitos de resultado o de mera actividad, y qué consecuencias se desprenderán de ello.

b.1. Elementos del artículo 264.1 CP.

Como es sabido, la parte objetiva de la conducta típica, que es la que ahora interesa, abarca un aspecto físico, o si se prefiere, externo. Además se precisa, en función del tipo de delito en el que estemos, un resultado lesivo para el bien jurídico, o por lo menos una puesta en peligro de ese bien protegido[449].

El apartado primero del artículo 264 CP establece que esa conducta externa que puede dar lugar a la aparición del tipo penal es la de *borrar, deteriorar, alterar, suprimir o hacer inaccesibles* datos, programas informáticos o documentos electrónicos. Como es habitual, además de estas posibles conductas nos encontramos con otra pluralidad de requisitos, siendo por tanto necesario para la posible concurrencia del tipo la concreción de estos otros elementos[450]. Éstos serán los de

[449] MIR PUIG, S.: *Derecho…* ob. cit. p. 219 y OCTAVIO DE TOLEDO Y UBIETO, E. y HUERTA TOCILDO, S.: *Derecho penal parte general. Teoría jurídica del delito*, Ed. Rafael Castellanos, 2ª edición, Madrid, 1986, pp. 76 y ss.

[450] No sólo es necesaria la aparición de los elementos externos sino, como veremos más adelante, también la concurrencia del tipo subjetivo o la inexistencia de causas de justificación por ejemplo. De todos modos, sí puede afirmarse que si la conducta analizada no presenta alguno de estos elementos externos entonces no estaremos ante una acción típica, siendo innecesario por tanto continuar con el análisis de otros extremos.

"por cualquier medio", "sin autorización" y "de manera grave". Además se exige la necesidad de producción de un resultado grave para la consumación del tipo.

Como hemos observado, la acción típica es aquella que consiste alternativamente en borrar, deteriorar, alterar, suprimir, o hacer inaccesibles datos, programas informáticos o documentos electrónicos ajenos. Descripción que es similar en lo sustancial a la que existía en el antiguo artículo 264.2 CP[451]. Se ha sustituido la expresión "destruir" por la de "borrar" y "suprimir", se ha eliminado la mención a "inutilizar" y se han añadido las de "hacer inaccesibles" y "deteriorar". Los cambios no suponen una modificación importante, sino que subyace en la idea del legislador adaptar lo más fielmente posible el texto de la Decisión Marco 2005/222/JAI a nuestro Código[452].

b.1.1. Las acciones de borrar y suprimir datos, programas informáticos o documentos electrónicos.

A nuestro juicio es acertada la sustitución de la expresión "destruir" por la de "borrar" y "suprimir", dado que desde una perspectiva semántica se habla de daños sobre objetos inmateriales[453]. Mientras que la acción de destruir parece enfocada a la desaparición física de un objeto material, las acciones de borrar o suprimir tienen un encaje más apropiado en el campo de la informática, donde, en principio, no es la destrucción física del objeto la que produce el daño, ni siquiera en los casos en los que la destrucción física del *hardware* supone el daño sobre los datos, programas informáticos o documentos electrónicos, pues esa acción entrará en la mayoría de los casos dentro de "hacer inaccesibles" los datos, pero no quedará necesariamente subsumida en las anteriores[454]. En todo caso, debemos entender superada la

[451] Artículo 264.2 CP (anterior a la reforma): "La misma pena se impondrá al que por cualquier medio destruya, altere, inutilice o de cualquier otro modo dañe los datos, programas, o documentos electrónicos ajenos contenidos en redes, soportes o sistemas informáticos"

[452] DE LA MATA BARRANCO, N. J.: "El delito…" ob. cit. p. 161.

[453] Se aprecia, de entrada, una diferencia sustancial entre los daños clásicos y los daños informáticos, pues el objeto material es de diferente naturaleza, lo que va a provocar problemas de interpretación del concepto, así ABOSO, G. E. y ZAPATA, M. F.: *Cibercriminalidad y Derecho penal*, Ed. B de F, 1ª edición, Montevideo, 2006, p. 75.

[454] La destrucción física de alguna de las piezas fundamentales que hacen funcionar un sistema informático -placa base, microprocesador o memoria RAM entre otros- puede convertir en inaccesibles ciertos datos informáticos. Sin embargo, si el daño físico no ha afectado al dispositivo

interpretación que sobre la destrucción se hace en el derecho clásico de daños -en el ámbito penal- según la cual se contraponía la interpretación restringida del daño penal en la que sólo el menoscabo o la destrucción llevaban aparejadas la aparición de la acción típica y el daño en su sentido más amplio, que extendía el daño penalmente relevante también al menoscabo del valor de uso del objeto, pues es, precisamente, sobre este eje sobre el que gira el daño informático[455].

Cuestión más importante es si realmente nos encontramos ante acciones iguales, o borrar y suprimir pueden entenderse como dos acciones diferentes. Nada se dice sobre esta cuestión en la doctrina, y en función del significado que se dé a estos términos, podemos estar ante acciones que suponen conductas de mayor o menor desvalor para el bien protegido, lo que comporta que no deban ser tratadas de la misma manera por los tribunales cuando llegue el momento de individualizar la pena a imponer. Determinadas interpretaciones podrían incluso convertir en atípicas ciertas conductas aparentemente típicas.

Si nos detenemos en la definición que de los vocablos "borrar" y "suprimir" realiza la Real Academia Española (en adelante RAE), encontramos que mientras por el primero se entiende "hacer desaparecer por cualquier medio lo representado con tiza, tinta, lápiz, etc." y "desvanecer, quitar, hacer que desaparezca algo"; suprimir se define como "hacer cesar, hacer desaparecer" y "omitir, callar, pasar por alto". De la lectura de ambas definiciones, por lo menos desde el sentido que les otorga la RAE, se nos presentan ambas palabras como sinónimas. La realidad es que, en el caso que nos ocupa, acudir a la definición que la RAE facilita resulta equívoco por varios motivos. En primer lugar, porque no debemos olvidar que la descripción de la acción típica viene de la traducción del inglés, que es el idioma en el que originariamente se

---

concreto donde se encuentran almacenados, la integridad de estos datos no se habrá visto comprometida, sino exclusivamente su posible acceso.

[455] En general la doctrina ha venido a utilizar, ya para los daños clásicos del artículo 263 CP, la interpretación amplia de daño que implica tanto a la esfera física del objeto como a su utilidad, véase SANTA CECILIA GARCÍA, F.: *Delito de daños. Evolución y dogmática (art. 263 Código penal)*, Ed. Universidad Complutense de Madrid, 1ª edición, Madrid, 2003, p. 230, BAJO FERNÁNDEZ, M.: *Compendio de Derecho penal. Parte Especial (volumen I)*, Ed. Centro de Estudios Ramón Areces, 1ª edición, Madrid, 1998 pp. 505 y 506 o RODRÍGUEZ DEVESA, J. M. y SERRANO GÓMEZ, A.: *Derecho penal español. Parte Especial*, Ed. Dykinson, 18ª edición, Madrid, 1995, p. 384.

decidió sancionar tales conductas[456], en el que de forma parecida a lo que ocurre con la lengua española, se confunde lo que se entiende por borrar (*delete*) con suprimir (*suppress*). Sin embargo, si el legislador internacional, luego el europeo, y finalmente el español han mantenido ambas acciones como diferenciadas en la redacción del tipo es porque se pretenden cubrir situaciones que no son exactamente iguales. Por lo menos podemos afirmar que eso pretendió el Convenio de Ciberdelincuencia de 2001, que es el que originariamente reguló la materia objeto de investigación. Que la traducción literal de los términos en nuestra lengua sea la más adecuada para reflejar el desvalor de cada conducta es algo que se puede discutir.

Para resolver esta cuestión nos vemos en la necesidad de acudir a entornos más técnicos, alejados del purismo de los diccionarios clásicos y normalmente varios pasos por delante de éstos en cuanto a tecnología se refiere. Sin todavía diferenciar entre la acción de suprimir y la de borrar, podemos decir que existen por lo menos dos maneras de conseguir que una serie de datos desaparezcan, al menos aparentemente, de un sistema informático[457]. Cuando se hace que desaparezcan unos datos de un sistema informático pueden haber ocurrido dos cosas:

1. Que no se hayan eliminado los datos del disco o soporte sobre el que se hayan almacenado, sino que realmente se haya ejecutado una orden del sistema informático que marca que los sectores ocupados por ese dato en la superficie del disco están disponibles para siguientes reescrituras, de tal forma que la representación visual para el usuario, que es la que se nos muestra a través de un monitor o *display*, revele que no existen datos (es lo que coloquialmente se llama borrar o suprimir un archivo). En este caso los datos no han desaparecido del *hardware*, sino que su representación visual no aparece. Se puede acceder a esos datos con *software*

[456] El artículo 5 del Convenio de Ciberdelincuencia de 2001, en el que tiene origen la redacción de la Decision Marco 2005/222/JAI, y posteriormente la regulación española, establece en su redacción que: *"Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the damaging, deletion, deterioration, alteration or suppression of computer data without right."*

[457] Aunque sobre ello volveremos al hablar sobre el objeto material de estos delitos, baste ahora señalar que los documentos electrónicos son datos informáticos también, y los programas informáticos son igualmente una serie ordenada de varios miles o millones de datos informáticos; por lo tanto, aquello que digamos ahora para los datos es igualmente aplicable a documentos electrónicos y programas informáticos.

específico salvo que sobre ese sector del disco se hayan sobrescrito otros datos posteriormente. Por lo tanto, a excepción de que exista la mencionada reescritura con nuevos datos, los datos anteriores quedan alterados de tal manera que pueden resultar inaccesibles, si bien siguen manteniendo su existencia.

2. Que realmente se haya dado una orden al sistema informático para reescribir el sector donde se encontraban los datos para dejarlo sin contenido (lo que se llama un borrado de bajo nivel). En este caso los datos han desaparecido del dispositivo y su recuperación es extremadamente complicada o imposible. Han dejado de existir. Por tanto, a diferencia del ejemplo anterior, no estamos ante una mera técnica para hacer inaccesibles los datos, si no que estamos realmente ante la desaparición real (inexistencia) de dichos datos.

Lo que queda preguntarnos desde este momento es si las dos acciones descritas pueden ser indicativas de lo que el legislador pretendía al separar las figuras de *"borrar"* y de *"suprimir"* en la redacción del tipo. Aunque en los círculos técnicos también se confunden ambos vocablos a la hora de referirse a estas acciones diferentes, existe una aceptación mayoritaria para entender que, en sentido estricto, el primero de los casos que exponíamos, el que hacía desaparecer el dato de la representación gráfica, pero conservaba su integridad y podía ser recuperado sin excesivos problemas mientras no existiese una sobrescritura en el mismo sector del dispositivo de memoria donde se almacena, se considera borrar un dato. Por el contrario, cuando no sólo se hace desaparecer el dato de la representación visual o vía de acceso habitual del sistema sino que además desaparece del soporte y se vuelve irrecuperable, entonces nos encontramos ante un dato suprimido[458]. Siendo estas las premisas, creo que se debe aceptar como correcta la idea de que el legislador, a la hora de diferenciar la acción de borrar y la de suprimir, tenía en mente una concepción similar a la expuesta. Este extremo es importante porque no

[458] La palabra *delete*, traducida del inglés como borrar, significa eliminar texto, datos o documentos, con el matiz de que cuando se borran esos archivos no se están suprimiendo del soporte, pero el espacio que están ocupando en el mismo se habilita para otros datos. Es una instrucción del sistema operativo para que ignore el archivo a través de un comando específico que se añade a la cabecera del archivo. S.M.H COLLIN: *Dictionary of computing*, Ed. Blomsbury Publishing, 5ª edición, Londres, 2004, p. 98. La palara s*uppress*, traducida como suprimir, que no tiene una acepción específica en informática, significa eliminar y supone la desaparición total del objeto, su inexistencia.

son acciones equivalentes, sino realmente conductas bien diferenciadas, en las que el sujeto activo se comporta de diferente manera, y además, tiene que llevar a cabo diferentes actuaciones para conseguir uno u otro efecto sobre los datos en función de lo que pretenda. Baste decir que la acción de suprimir es más compleja y, por lo menos en la actualidad, requiere de unos conocimientos que, si bien no son demasiado complejos ni difíciles de conseguir, no son de conocimiento general. A diferencia de ello, todo el mundo conoce la forma de borrar un archivo (la clásica opción de eliminar de los sistemas informáticos). Además, como se expuso anteriormente, la supresión del dato es prácticamente irreversible, mientras que el dato borrado puede ser, en ocasiones, de extremadamente fácil recuperación, aunque es cierto que en otras situaciones las consecuencias pueden resultar similares a las del suprimir.

b.1.2. La acción de hacer inaccesibles datos, programas informáticos o documentos electrónicos.

Sobre la sustitución de la acción "inutilizar" por la de "hacer inaccesibles" se plantea una situación más compleja de lo que parece, pues no se está ante un acomodo lingüístico, sino ante una verdadera ampliación de las barreras de protección que establece el tipo penal[459]. La expresión inutilizar entendida como la imposibilidad de practicar el uso habitual para cuyo fin existía el objeto material se ve superada por la de "hacer inaccesibles", en la que los datos pueden no haber sido inutilizados, pues en caso de acceder a los mismos su funcionalidad o información siguen intactos, pero el atacante se ha procurado de un método para que no se pueda acceder a dichos datos, de tal forma que, como la expresión establece, se ha hecho inaccesible[460]. Otra interpretación posible, aunque semánticamente menos correcta, es la de entender que la inaccesibilidad de los datos, programas informáticos o documentos electrónicos equivale a su inutilidad por cuanto, con dicha imposibilidad de acceso no se está sino impidiendo dar a los datos, programas informáticos o documentos electrónicos la utilidad para la que fueron creados, y en consecuencia, se

[459] DE LA MATA BARRANCO, N. J.: "El delito…" ob. cit. p. 162.

[460] O como se refiere DE LA MATA BARRANCO, N. J.: "El delito…" ob. cit. p. 162. "ahora con la expresión "hacer inaccesibles" más amplia […] puede incluir el establecimiento de barreras que impidan llegar a datos que no se han afectado".

encuentran inutilizados. Esta segunda interpretación es menos precisa que la expuesta en primer término, como veremos a continuación

Resulta importante la introducción de esta barrera, anterior a la producción real de un daño sobre datos, programas o documentos, puesto que una considerable cantidad de virus informáticos y otra serie de *software* malicioso no tienen por objeto la afectación del contenido de los datos, sino simplemente procurarse la inaccesibilidad a los mismos[461]. Ahora bien, aquel *software* que impide el acceso a cierto tipo de datos normalmente no lo hace de forma permanente, es decir, si esos datos pueden ser ejecutados en otro sistema informático diferente y en ese nuevo equipo el acceso está habilitado, o incluso en el caso de que en el sistema informático original, con un *software* alternativo pueda eliminarse la inaccesibilidad volviendo a quedar los datos en su estado original, se pueden plantear problemas de tipicidad, pues resultaría comprometido afirmar que se ha producido el resultado o por lo menos la puesta en peligro del bien jurídico. Pero existe una tercera alternativa, que es la alteración de los propios datos modificando su contenido, para convertirlos en inaccesibles. A este respecto existen cuestiones que se deben resolver.

En el primer y segundo caso, cuando el simple hecho de ejecutarse los datos en un sistema diferente o utilizando otro *software* de limpieza ya se permite el acceso a los mismos, podríamos preguntarnos si la acción típica se ha producido; lo que suscita la necesidad de encontrar solución al problema de la temporalidad. Y en el tercer ejemplo, cuando los datos se han convertido en inaccesibles alterando los propios datos pero sin afectar a la información contenida en ellos, no estaríamos ante la acción "hacer inaccesible" sino más adecuadamente por el propio significado de

[461] Es frecuente que un virus instalado en un sistema informático no dañe determinados tipos de archivos, como pueden ser por ejemplo los documentos de texto, pero impide al sistema abrir ninguno de esos documentos de tal forma que si esos mismos documentos fueran extraídos de ese sistema informático e introducidos en otro, su acceso y funcionalidad seguirían intactas, pues aquello que los ha hecho inutilizables no ha sido un daño sobre los mismos, sino una técnica que afecta a su accesibilidad (no a su integridad). Una cuestión que debe ser debatida es hasta qué punto es punible la acción de hacer inaccesibles ciertos datos, programas informáticos o documentos electrónicos, cuando se realiza tal acción por medio de estas técnicas, ya que con el simple hecho de ejecutar tales datos en otros sistemas informáticos los mismos volverán a ser accesibles. No debemos olvidar en todo caso que la acción del virus de este ejemplo sería una acción típica en sí misma, pues para evitar que un sistema ejecute determinados documentos debe alterar el contenido de ciertos datos (ajenos normalmente a los propios documentos) para conseguir el resultado de hacerlos inaccesibles, lo que nos llevaría a plantear ciertos problemas concursales a los que nos referiremos más adelante.

las palabras, ante la acción de "alterar"[462]. Expuestos estos extremos debemos afirmar que la inaccesibilidad típica a los datos, programas informáticos y documentos electrónicos siempre va a depender de acciones que se producen ajenas a la integridad de los datos, programas informáticos y documentos electrónicos en sí mismos, debido a lo cual, retomamos el asunto de la temporalidad en cuanto a la inaccesibilidad a los datos.

El precepto, como se observa, no se refiere a las consecuencias de hacer inaccesibles los datos, programas informáticos y documentos electrónicos sólo durante un periodo de tiempo, sea determinado o indeterminado. Aparte de esto, la doctrina confunde incompresiblemente el hecho de hacer inaccesibles datos, programas informáticos y documentos electrónicos (acción en el artículo 264.1 CP y medio para realizar la acción en el 264.2 CP) con el de obstaculizar o interrumpir un sistema informático (acciones del artículo 264.2 CP), tratando de equiparar una acción a otra cuando desde un punto de vista técnico y jurídico-penal son acciones bien diferentes[463]. Aunque del análisis de la figura del artículo 264.2 CP nos ocuparemos más adelante, baste ahora señalar que el objeto material de las figuras de los apartados primero y segundo son sustancialmente diferentes. Mientras que en el primero el objeto material son los datos, programas informáticos y documentos electrónicos, de manera que sólo estos sufren la acción de ser borrados, dañados, deteriorados, alterados, suprimidos o convertidos en inaccesibles; en la figura del apartado segundo el objeto material es un sistema informático (y no los datos, que se convierten en este caso en el modo a través del cual afectar a ese sistema informático) que se ve obstaculizado o inutilizado. No es, por tanto, lo mismo hacer inaccesible unos datos (art. 264.1 CP) que un sistema informático en su totalidad (art. 264.2 CP).

[462] Técnicamente se pueden alterar unos datos sin afectar al contenido preexistente, simplemente añadiendo nuevos datos que no afectan a la integridad de la estructura previa, pero que se suman a la misma.

[463] Así se desprende de la lectura de DE LA MATA BARRANCO, N. J.: "El delito…" ob. cit. p. 163, conforme a la cual "en la interpretación tradicional del delito de daños, cuando el objeto puede volverse a utilizar de modo absolutamente similar a como se usaba antes del ataque producido […] nadie afirmaba la tipicidad del mismo […] La cuestión es si con ello se satisfacen los compromisos internacionales adquiridos y se atiende a la realidad actual y el hecho innegable de que puede ser mucho más importante […] una imposibilidad temporal de utilización del sistema de cierta entidad que un mínimo menoscabo permanente".

Sentada esta diferencia y volviendo a la idea de la temporalidad de la inaccesibilidad los datos (y no la inaccesibilidad a un sistema informático) entendida sólo como la inaccesibilidad producida por un artificio externo al dato que no altera su contenido[464], creemos que la mejor forma de tratar esta situación es utilizar una solución inversa a la que se ha ofrecido por la doctrina para la figura de los daños del artículo 263 CP, en la que, si el objeto podía volverse a usar de la misma manera que antes de haber sido inutilizado, entonces sólo nos encontrábamos ante un perjuicio perseguible por la vía civil, pero no ante la conducta típica[465]. Tal como hemos definido la inaccesibilidad, esto es, como por artificio externo a la sustancia de los datos, excluyendo la inaccesibilidad por alteración de los propios datos; lo correcto es decir que toda imposibilidad de acceso, cuando sigue este esquema propuesto, es temporal, pues los datos no han sido deteriorados, alterados, borrados o suprimidos y siempre podrán por tanto volver a ser accesibles a través de unas u otras técnicas. De tal manera que el legislador lo que ha pretendido precisamente con la introducción de esta regulación es un tipo penal que castigue no sólo el daño a los datos, sino además, que a unos datos a los que no se les ha dañado en sentido estricto, se les impida el acceso. Configurada de esta forma, como se puede observar, la acción "hacer inaccesible" no tiene el mismo significado clásico que se le ha otorgado a la acción "inutilizar", por cuanto en el caso actual la temporalidad no es una causa de exclusión de la tipicidad como la inutilidad en los daños clásicos, sino un elemento necesario de la propia acción de hacer inaccesible, porque de lo contrario deberíamos subsumir estas conductas en las de deterioro, con la consiguiente discusión doctrinal sobre la temporalidad. Temporalidad por tanto que el legislador ha decidido castigar, pues ella es la nota característica de hacer algo inaccesible. Contra esta interpretación cabría aludir a la incongruencia del propio precepto en el Código penal, pues como ya hemos avanzado en el apartado dedicado al bien jurídico protegido -y será extensamente tratado en el siguiente capítulo- si nos encontramos ante el bien jurídico patrimonio, y sólo deben ser sancionadas aquellas acciones que directamente menoscaban el patrimonio de un sujeto, podríamos preguntarnos si entonces el mero

[464] La inaccesibilidad producida por la alteración de la propia sustancia del dato debe ser considerada como una alteración y así será tratada en este trabajo.

[465] Está postura la defiende con matices DE LA MATA BARRANCO, N. J.: "El delito…" ob. cit. p. 163.

hecho de hacer inaccesible algo como aquí ha sido planteado no afecta directamente al patrimonio del sujeto por cuanto en caso de que la inaccesibilidad cese, el perjuicio patrimonial directo no ha existido (aunque pueda considerarse un lucro cesante, o un gasto en la reparación, cuestiones que como veremos deben ser excluidas del daño en el ámbito penal) y, por lo tanto, si no se lesiona el bien jurídico, no existiría delito.

b.1.3. La acción de alterar datos, programas informáticos o documentos electrónicos.

Otra acción importante recogida en el tipo del artículo 264.1 CP es la de "alterar", sobre cuyos límites también es necesario realizar el oportuno análisis. En principio, alterar puede entenderse como modificar o cambiar la esencia de algo. Y en ese sentido alterar datos, programas informáticos o documentos electrónicos no tiene necesariamente que conllevar el menoscabo de su funcionalidad o, en general, implicar un daño para los mismos. De ahí que parte la doctrina se pregunte si, por ejemplo, añadir nuevos datos a los existentes pero sin eliminar los datos previos, de tal forma que coexistan los anteriores y los posteriores, es decir, sin que se haya alterado el contenido original en el sentido más amplio de la palabra, puede suponer o no que nos encontremos ante una acción típica[466].

De lo que no parecer haber duda es de que la alteración de datos, programas informáticos o documentos electrónicos se puede realizar a través de dos acciones: aumentando la sustancia los mismos (es decir añadiendo nuevos datos al conjunto), o bien disminuyéndola. Otra clasificación posible, a nuestro juicio más acertada, es aquella que diferenciaría entre las alteraciones constructivas y las destructivas; basada esta segunda en el aumento o disminución del valor económico, independientemente de que se aumente o disminuya la sustancia de los datos, programas informáticos o documentos electrónicos. Mientras que en la primera clasificación, aquella que distingue según aumente o disminuya la sustancia, se interesa la forma por la que se alteran los datos, donde no toda modificación que aumente o disminuya la sustancia de los datos, programas informáticos o documentos electrónicos tiene porque ser típica; la segunda clasificación, que

[466] DE LA MATA BARRANCO, N. J.: "El delito…" ob. cit. p. 163.

diferencia entre alteraciones constructivas y destructivas, trata de separar las alteraciones en dos grupos: uno en que se mantiene o se aumenta la utilidad propia de los datos, programas informáticos o documentos electrónicos (que se haya aumentado o se haya disminuido su sustancia, es ahora intrascendente); y un segundo grupo de casos en los que se ha disminuido su funcionalidad (se haya producido una introducción de sustancia o eliminando parte de la misma). Esta bipartición nos permite afirmar que será siempre típica la alteración destructiva, mientras que la constructiva no debería serlo. Sin embargo, a pesar de resultarnos más apropiada está clasificación, tampoco está exenta de problemas ya que la apreciación de cuándo una alteración encaja en uno u otro grupo puede resultar, caso por caso, complicada.

Para analizar estas cuestiones se debe aclarar que, tal y como se encuentra encuadrado este delito en nuestro Código penal, nos encontramos en el Capítulo dedicado a los daños, y por tanto, y a salvo de futuras precisiones, el bien jurídico protegido por estos preceptos en general es el patrimonio. Puntualizamos este hecho porque no creemos que el bien jurídico sea tanto la integridad o utilidad de la cosa, como sí lo es su valor económico (delitos contra el patrimonio). Visto así, parece difícil entender como daño en sentido patrimonial y en el ámbito de la informática, una acción que mejore o por lo menos no disminuya el valor económico de la cosa objeto de la acción, aunque sí modifique la sustancia de la misma. Traducido al caso que se analiza, alterar datos de tal forma que el valor económico de lo modificado no se vea mermado y, más aún en el caso de que el valor económico se vea aumentado (por ejemplo introduciendo funcionalidades a un programa, o añadiendo información correcta a un documento electrónico), no puede constituir la acción típica del artículo 264.1 CP[467].

[467] Este punto de vista puede parecer enfrentado con la visión clásica del delito de daños del artículo 263 CP en el cual desde el momento en que se produce un daño sobre un objeto con valor económico se produce el daño, aunque como resultado del mismo se produzca un beneficio patrimonial para el propietario -se utiliza el ejemplo clásico de un solar en el que existe un edificio en ruinas, el cual es destruido por la acción de un tercero, aumentando el valor de dicho solar en el mercado a pesar de los daños sobre la estructura del viejo edificio-. Entre otros, SANTA CECILIA GARCÍA, F.: *Delito*… ob. cit. p. 269, "Ahora bien, cuando hablamos del valor de la cosa nos referimos al que tuviera ésta al tiempo de su destrucción o menoscabo (daño genuino) en su objetiva estimación pericial judicialmente aceptada, y no al resultado patrimonial último". Este razonamiento, posible en el caso de los daños clásicos del artículo 263 CP, queda limitado en el ámbito de los daños informáticos del artículo 264.1 CP desde el momento en que en realidad nunca existe una destrucción

Dicho esto, a continuación vamos a tratar de identificar qué acciones pueden verse subsumidas en la de "alterar". Como se ha expresado en líneas anteriores, cuando nos referíamos a la acción de "hacer inaccesibles", una primera forma de alterar los datos, documentos o programas informáticos puede ser la de procurarse la inaccesibilidad de los mismos a través de una alteración en la propia sustancia de los datos, programas informáticos o documento electrónicos (no por medio de modificaciones externas). Como se ha expresado anteriormente, si bien el resultado es que los datos se hacen inaccesibles, lo que ha motivado dicha inaccesibilidad ha sido la alteración de los propios datos, es decir, el *iter* se desarrolla de forma lineal: primero se altera, y ello produce que se haga inaccesible. En nuestra opinión, por tanto, no estamos ante una acción de "hacer inaccesible" sino ante una auténtica acción de "alterar", que se sujeta perfectamente a la definición de alteración que se refirió con anterioridad, pues no cabe duda de que dicha alteración supone un menoscabo del valor patrimonial de los datos, programas informáticos o documentos electrónicos.

En segundo lugar, puede que la alteración de los datos se produzca eliminando parte de la información que contienen los propios datos, programas informáticos o documentos electrónicos. En este caso pueden producirse dos consecuencias. Que la eliminación de esa parte del todo no suponga un perjuicio en el valor económico de los datos, programas o documentos, por ejemplo, se elimina parte del código fuente de un programa que resultaba innecesario; o por el contrario, que la eliminación de esa parte suponga a su vez que los datos, programas o documentos pierdan parte de su utilidad original. Parece lógico que, atendiendo a las mismas razones que ya exponíamos respecto a la afectación o no del bien jurídico protegido, si la alteración consistente en eliminar una parte de los datos, programas o documentos no afecta a utilidad final, será difícil aceptar la tipicidad del hecho al ser complicado comprobar la disminución de su valor económico. Cuestión diferente es

---

física de objetos, sino que el ámbito gira sólo en torno a la utilizad del bien que queda estrechamente ligada, ahora sí, con el perjuicio causado. Si la alteración no produce disminución de la utilidad de los datos informáticos no habrá daño en sentido típico, y además no existirá perjuicio. En cambio siempre que la alteración disminuya la utilidad, además de producir un perjuicio, se producirá la acción típica. La vinculación daño-perjuicio queda por tanto estrechamente ligada, diferencia sustancial con el caso de los daños tradicionales.

la que se suscita cuando sí que se afecta a la utilidad, y por tanto consiguientemente a su valor patrimonial. En este último caso parecería obvio entender que la conducta es subsumible en el tipo.

Más allá de esta lógica separación, se plantean dudas en cuanto a la similitud entre la acción de alterar suprimiendo parte de la sustancia de los datos, programas o documentos, con la acción de "deteriorar" datos, programas informáticos o documentos electrónicos, que en la concepción tradicional se configura como el menoscabo de la cosa[468], es decir, la pérdida de sustancia de la misma que conlleva una afectación a su valor económico. Parece que así entendido nos encontraríamos ante una acción análoga a la de alteración en los datos, programas informáticos o documentos electrónicos, cuestión que abordaremos más adelante.

Una tercera modalidad de alteración, y la que más problemas de interpretación puede causar tanto en sede judicial como en la doctrina, va a ser aquella que modifica los datos, programas o documentos, y sin embargo no elimina su función o información original, pero modifica su contenido o estructura. En este caso, como avanzábamos en líneas precedentes, se debe atender la afectación del valor económico de los datos, programas informáticos o documentos electrónicos. Este es un problema que los tribunales y la doctrina deberán resolver caso por caso, como vamos a explicar a continuación.

Efectivamente, puede haberse modificado la estructura de los datos y que estos conserven intacta la funcionalidad que tenían antes de la modificación, pero será complicado resolver si esa nueva estructura responderá igual de bien (o de mal) ante los diferentes usos que se le vaya a dar, usos por otro lado indeterminados. No se debe olvidar la complicación propia del ámbito de la informática, donde nos referimos, por lo menos en todos estos supuestos, siempre a objetos inmateriales. En el caso de un programa informático, sin ir más lejos, no siempre es correlativo el hecho de aumentar la funcionalidad del mismo con aumentar su valor económico[469].

[468] SANTA CECILIA GARCÍA, F.: *Delito*… ob. cit. p. 243 y ANDRÉS DOMÍNGUEZ, A.C.: *El Delito*... ob. cit. p. 128.

[469] MUÑOZ CONDE, F.: *Derecho Penal, Parte Especial*, Ed. Tirant lo Blanch, 18ª edición, Valencia, 2010, p. 476, en el ámbito de los daños clásicos del artículo 263 CP, plantea qué ocurre cuando un daño sobre un objeto produzca en realidad un beneficio económico al propietario de dicho objeto

Precisamente, los programas más especializados, con pocas funcionalidades generales, son los más caros en el mercado[470]. Lo mismo podemos afirmar con respecto a los documentos electrónicos: es cierto que una tabla en la que se recogen, por ejemplo, códigos postales, puede ser alterada para añadir aquellos que faltaban o corregir aquellos que estaban mal, y en ese caso parece claro que la conducta sería atípica. Pero no todos los casos son tan claros. Piénsese aquella situación en el que se aumenta la sustancia de un documento electrónico que contuviera la única copia del borrador de una novela de un autor de reconocido prestigio: incluso si dicha modificación por la que se aumenta su sustancia tuviera una calidad narrativa mejor que la del autor original, el hecho de tener un origen ajeno al mismo produciría que ese documento electrónico perdiera valor económico -cuando podría incluso afirmarse que objetivamente se ha mejorado-.

Estos son sólo algunos ejemplos simples de la amplia casuística que este término de "alterar", referido a modificar, puede originar en la práctica real. Incontables son las posibilidades y la única solución que podemos dar ahora es la de esperar a que doctrina y jurisprudencia se pronuncien sobre cada caso en particular, de tal forma que se puedan sentar unas bases interpretativas generales.

b.1.4. La acción de deteriorar datos, programas informáticos o documentos electrónicos.

La penúltima acción que se debe analizar es la referida a "deteriorar", acción a la que ya hemos aludido anteriormente cuando nos referíamos a la acción de "alterar". La concepción clásica del deterioro en los delitos de daños ha sido la de estropear, o menoscabar el objeto. Claro que en los casos que nos ocupan ese objeto tiene un carácter inmaterial, lo que nos lleva a preguntarnos cuándo se produce un menoscabo en los datos, programas informáticos o documentos electrónicos, o

(muerte de un animal enfermo o el derribo de una casa en ruinas), concluyendo que en todo caso, existirá el daño típico pues aunque el patrimonio del propietario, en general, puede verse beneficiado, la cosa objeto de la acción de dañar tenía un valor individualizable, que en todo caso habrá perdido.

[470] Los programas más especializados en materias concretas, como Autocad o Photoshop pueden rondar en torno a los 1.000 dólares el precio del paquete básico, pudiendo elevarse hasta más allá de los 100.000 dólares en caso de paquetes profesionales.

incluso, si lo que sería el deterioro informático ya ha quedado subsumido dentro de otras acciones tipificadas en el mismo artículo, como parece lo más probable.

Señala la doctrina que el deterioro en los delitos de daños clásicos se entiende como aquel ataque que no ha llegado a producir la destrucción de la cosa, pero que ha provocado una modificación resultado de la cual la cosa, aunque sigue existiendo, ha perdido parte su valor económico[471]. Establecida esta definición para la acción de deteriorar, no cabe duda de que puede ser igualmente válida para el tipo del actual artículo 264.1 CP, con la salvedad de que nos encontramos ante bienes de carácter inmaterial, aunque igualmente con un contenido determinado sobre el que se puede analizar la existencia o no de una modificación.

Sin embargo, y a la luz de lo manifestado respecto del resto de las acciones tipificadas, no aporta contenido adicional la conducta consistente en deteriorar datos, programas informáticos o documentos electrónicos cuando se ha introducido como típica la alteración de los mismos, que es una acción más general. Así, el alterar engloba la acción de deteriorar, porque según la clasificación que realizábamos al respecto entre modificaciones constructivas (que aumentaban o mantenían el valor de los datos, programas o documentos) y modificaciones destructivas (que hacían perder valor económico), el deterioro se encontraría dentro de las segundas, concretamente en aquellas en las que además de perder valor económico se pierde sustancia de la cosa. Y como veíamos en ese mismo apartado, dichas acciones de alteración, las destructivas, serían siempre acciones típicas.

b.1.5. La acción de dañar datos, programas informáticos o documentos electrónicos.

Por último queda analizar la acción de "dañar", que se configura en el tipo como otra forma de daño sobre los datos, programas informáticos o documentos electrónicos[472]. En este caso nos encontramos ante una acción que parece haber quedado vacía de contenido a tenor del resto de acciones reguladas. Acudiendo a la doctrina general del delito de daños, nos encontramos nuevamente con la idea de que

[471] SANTA CECILIA GARCÍA, F.: *Delito…* ob. cit. pp. 230 y ss. y ANDRÉS DOMÍNGUEZ, A.C.: *El Delito…* ob. cit. p. 128.

[472] DE LA MATA BARRANCO, N. J.: "El delito…" ob. cit. p. 161.

el daño en el ámbito penal se produce por la lesión de la integridad de la cosa, o bien por su destrucción o inutilidad, que llevan aparejado a su vez un perjuicio económico[473]. Esta construcción que realiza la doctrina parece acertada por cuanto en el artículo 263 del Código penal no se hace, a diferencia de lo que ocurre en el artículo 264.1 del mismo, una enumeración de las posibles acciones que pueden producirse sobre el objeto material. Por tanto, la doctrina, en su inestimable labor, establece el contenido y significado que debe darse el daño clásico, siendo éste el ya apuntado: destrucción, deterioro e inutilidad.

La cuestión que nos queda resolver por tanto, es si el daño que se recoge en el artículo 264.1 CP como una acción más destinada a afectar a la integridad y funcionalidad de los datos, programas informáticos o documentos electrónicos tiene un contenido diferente al que comporta en la figura clásica del artículo 263 CP y, en caso afirmativo, analizar cuál es la diferencia con éste, y cuáles son las diferencias con el resto de acciones recogidas en el artículo 264.1.

Partiendo del hecho de que la expresión "dañar" es la más general de las acciones del artículo 264.1 CP, al igual que ocurre con el desarrollo que se ha seguido hasta este punto, debemos dotar de contenido a dicha acción, pues así enunciada resulta excesivamente amplia. Pero para ello resulta muy difícil escapar a la definición que de dañar se realiza por la doctrina cuando se refiere a los daños en las cosas del artículo 263 CP, contenido que no se extrae de una compleja discusión, sino de una más o menos uniforme aplicación de la semántica de la propia palabra, que se circunscribe, o bien a la destrucción, o bien al deterioro o la inutilización. Extrayendo esta tesis que hoy no es discutida por los autores ni la jurisprudencia[474], no parece que pueda darse otro significado a la acción de "dañar" del artículo 264.1 CP. De tal forma que lo que se está castigando realmente es destruir, deteriorar o inutilizar datos, programas informáticos o documentos electrónicos. Ahora bien,

[473] SANTA CECILIA GARCÍA, F.: *Delito*… ob. cit. pp. 234 y 235 y ANDRÉS DOMÍNGUEZ, A.C.: *El Delito*… ob. cit. p. 128.

[474] SANTA CECILIA GARCÍA, F.: *Delito*… ob. cit. p. 235, señala que "la bibliografía resalta el contenido del artículo 265 del Código Penal en el que se especifica la conducta típica del delito de daños: destruir, dañar de modo grave o inutilizar para el servicio", para concluir respecto de la falta de definición de daño del artículo 263 CP que "la distinción no tenga más valor que el puramente literario, sin permitir distingos entre las posibilidades típicas". También ANDRÉS DOMÍNGUEZ, A.C.: *El Delito*… ob. cit. p. 128.

analizando estas tres acciones de manera mucho más pormenorizada, y después del desarrollo que ya llevamos realizado, podemos extraer algunas mínimas conclusiones. En primer lugar, la acción de destruir en el ámbito de la informática, donde los objetos son inmateriales, no es la más adecuada, y debe ser sustituida como ya se señaló en su momento por la de "suprimir" (o en algunos casos la de "borrar"). En segundo término, la acción de deteriorar, con la crítica que se apuntaba, ya se encuentra recogida literalmente en el tipo penal. Y por último, la acción de inutilizar, como también se ha explicado, ha quedado subsumida bajo la acción de "hacer inaccesibles", pues esta es más amplia que la anterior, pero la engloba igualmente.

Sobre estos extremos volveremos en la tercera parte de la investigación. Baste ahora sugerir que la acción de "dañar" parece resultar una acción vacía de contenido en el actual artículo. De todo lo expuesto anteriormente cabe preguntarnos si el legislador europeo o supra europeo ha tomado en consideración estas u otras interpretaciones de los términos, o por el contrario se ha limitado a introducir una serie de acciones que se pueden realizar sobre datos, programas informáticos o documentos electrónicos con la intención de evitar lagunas, pero con una aparente ausencia de criterio a la hora de elegir el catálogo de conductas recogidas.

b.1.6. La fórmula "por cualquier medio".

El legislador, apartándose en este caso de lo exigido por la Decisión Marco 2005/222/JAI de 24 febrero, ha decidido añadir como elemento típico respecto de las acciones ya descritas, la fórmula de "por cualquier medio". Esta fórmula ya existía en la anterior regulación y su significado e interpretación por tanto no es nueva para nuestra doctrina. Parece haber acuerdo en identificar dicha expresión con la creación de un delito de medios indeterminados[475], o una "técnica de *numerus apertus*"[476], lo que abre un abanico de posibilidades casi inabarcable. En este sentido se han determinado dos grandes grupos de medios, tratando de enumerar las diferentes posibilidades: no cabe duda de que el daño a los datos, programas informáticos y documentos electrónicos puede producirse tanto por un ataque físico como por un

[475] MIRÓ LLINARES, F.: *Delitos…* ob. cit. p. 161.

[476] DE LA MATA BARRANCO, N. J.: "El delito…" ob. cit. p. 161.

ataque lógico (informático)[477]. En cuanto a la producción de un daño físico sobre el *hardware* en el que se encuentran los datos, cabe destacar que a través de una única acción pueden producirse dos resultados diferentes: el daño producido sobre el propio *hardware* (por lo que podríamos estar ante un daño del artículo 263 CP) y el producido en los datos, programas informáticos o documentos electrónicos como consecuencia del primero. Aunque estos temas los abordaremos a la hora de analizar la casuística concursal, baste ahora mencionar que para que se realice la figura del 264.1 CP el dolo debería abarcar tanto dañar el *hardware* como los datos, programas o documentos en él insertos[478].

Se plantea por tanto en la doctrina si los daños del artículo 264 CP subsumen también los daños sobre el *hardware* -daños físicos- o deben ser reconducidos al artículo 263 CP[479], cuestión para la que no encontramos una respuesta contundente. No parece lógico, en todo caso, tratar de unir las dos figuras puesto que, precisamente, lo que pretende el artículo 264 CP es tutelar esa parte que quedaría desprotegida con la existencia única del artículo 263 CP, en la que sólo se protegen objetos físicos como es el *hardware*. El objeto material es sustancialmente diferente y, como se puede comprobar, la forma de vulnerar el bien jurídico protegido puede serlo también. Son cuestiones separadas, pudiendo producirse una acción del artículo 263 CP sin realizarse el tipo del 264 CP, o viceversa, o las dos a la vez: son por tanto figuras autónomas, en este caso el desvalor de la acción del 264.1 CP no cubre el desvalor del 263.1 CP[480].

---

[477] MIRÓ LLINARES, F.: *Delitos…* ob. cit. p. 161, al igual que DE LA MATA BARRANCO, N. J.: "El delito…" ob. cit. p. 161 hace la distinción entre ataques informáticos y ataques físicos. Pero va más allá en su enumeración, entendiendo que los ataques informáticos pueden ser tanto directos como remotos, e igualmente los ataques físicos pueden ser directos o indirectos.

[478] MIRÓ LLINARES, F.: *Delitos…* ob. cit. p. 161.

[479] ANDRÉS DOMÍNGUEZ, A. C.: "Daños" en ÁLVAREZ GARCÍA, F. J. y GONZÁLEZ CUSSAC, J. L. (dirs): *Comentarios a la Reforma Penal 2010,* Ed. Tirant lo Blanch, 1ª edición, Valencia, 2010, p. 294.

[480] El que tira al suelo un ordenador porque está enfadado con el dueño del mismo pretende dañar el ordenador como objeto físico, por su constatable alto valor económico, pero normalmente no estará pensando en los datos, programas o documentos que contiene ese ordenador. Puede ocurrir la situación inversa, aquel que está enfadado con otro entra su ordenador y suprime todos los datos existentes. Y una tercera vía, la que podría resultar de arrojar a una piscina un disco de almacenamiento externo para destruir los datos en su interior además de destruir físicamente el propio disco de almacenamiento.

La duda se plantea en torno al comportamiento material del autor, si cuando el artículo 264 CP hace referencia a cualquier medio, en realidad se limita a cualquier medio informático, y no a medios físicos de ataque a los datos, programas informáticos o documentos electrónicos[481]. A nuestro entender está consideración es errónea, por cuanto el artículo se limita a decir "cualquier medio", y extraer de la configuración del tipo penal que si los daños se producen en elementos lógicos, el medio para hacerlo debe ser exclusivamente a través de métodos informáticos desvirtúa el sentido literal del artículo. Será más correcta la interpretación extensiva[482] conforme a la cual el daño físico sobre el soporte es uno de esos medios posibles, siempre que el dolo abarque el daño sobre los datos, programas y documentos y no sólo el daño del *hardware*. Esta afirmación se ve reforzada por el hecho indiscutible de que el legislador al introducir la fórmula "por cualquier medio" pretende salvar cualquier duda respecto de cómo puede cometerse el delito. Si tal expresión no se hubiese introducido en el tipo penal por parte del legislador, podrían aparecer dudas sobre los medios comisivos. No obstante, tal circunstancia, en nuestra opinión, no debería alterar la interpretación que hemos realizado, aunque sí la haría más discutible que con su actual formulación[483]; la cual, como ya hemos apuntado, nos parece la más correcta.

b.1.7. La gravedad en el medio y la gravedad en el resultado.

A la expresión "por cualquier medio" añade el legislador dos elementos en la regulación que se configuran igualmente como necesarios. Nos referimos a la necesidad de que el daño -en sentido amplio- se produzca "de manera grave" y además que el resultado producido sea "grave".

---

[481] ANDRÉS DOMÍNGUEZ, A. C.: "Daños..." ob. cit. p. 294, señala que "si se entiende que el art. 264 queda circunscrito a los daños en los elementos lógicos de un sistema informático, los ataques a éstos, susceptibles de subsunción en el citado precepto, son los que se llevan a cabo, única y exclusivamente, a través de comportamientos informáticos y no a través de comportamientos físicos sobre su soporte".

[482] Apoyada por otros autores como se ha indicado anteriormente, véase MIRÓ LLINARES, F.: *Delitos...* ob. cit. p. 161 y DE LA MATA BARRANCO, N. J.: "El delito…" ob. cit. p. 161.

[483] Por ejemplo, el artículo 263 CP, al establecer que "el que causare daños en propiedad ajena…" no señala que esos daños se produzcan por cualquier medio, sin embargo no cabe duda en la doctrina, de que el medio para hacerlo puede ser cualquiera siempre que sea el idóneo para menoscabar, destruir o inutilizar el objeto. Véase ANDRÉS DOMÍNGUEZ, A.C.: *El Delito...* ob. cit. p. 151.

No es fácil valorar a que se refiere el legislador cuando se indica que la conducta se produzca "de manera grave"[484]. La mayoría de la doctrina ha decidido o bien pasar por alto esta doble gravedad exigida[485], o bien dar una explicación, a nuestro entender, poco convincente[486], o bien confundir la gravedad del comportamiento con la gravedad del resultado[487]. A nuestro entender es esta una forma errónea de interpretar el precepto, pues en la realidad puede ocurrir que una conducta poco grave -por ejemplo apagar un sistema informático pulsando la tecla de apagado cuando se debería apagar utilizando un comando del propio sistema[488]- produzca un resultado grave (borrado de todos los datos del sistema), e igualmente podría ocurrir que una conducta grave -golpear un ordenador con martillo- no produjese un resultado grave (no se llega a afectar la información del sistema). Por consiguiente, cuando el tipo penal exige que tanto la conducta como el resultado sean graves, lo configura como dos esferas diferenciadas y necesarias para la aparición de la conducta típica. A nuestro juicio, lo que el legislador ha tratado de expresar, es que no es válida cualquier forma de producir el daño en los datos, programas informáticos o documentos electrónicos, sino que la gravedad en el medio se puede configurar como límite a la fórmula anterior "por cualquier medio", de tal manera que será penalmente relevante cualquier medio siempre que fuera el idóneo para producir un daño informático cuyo resultado sea grave. En el ejemplo al que nos referimos antes, puede observarse que si bien la acción de apagar un sistema informático de golpe puede producir un resultado grave, no es la conducta idónea

[484] BARRIO ANDRÉS, M.: "La ciberdelincuencia…" ob. cit. p. 291, señala de entrada que la doble gravedad exigida en el tipo "se compagina muy mal con la seguridad jurídica".

[485] Es el caso de ANDRÉS DOMÍNGUEZ, A. C.: "Daños..." ob. cit. p. 294.

[486] MIRÓ LLINARES, F.: *Delitos...* ob. cit. p. 157, afirma que "no cualquier destrucción, alteración o inutilización de datos, programas o documentos electrónicos ajenos contenidos en redes, soportes o sistemas informáticos será delictiva y sancionable, con pena de prisión, sino sólo aquella que pueda reputarse grave".

[487] MIRÓ LLINARES, F.: *Delitos...* ob. cit. p. 161, señala que "tal exigencia típica resulta redundante si tenemos en cuenta que después se exige para la tipicidad que el resultado producido sea grave". En un sentido parecido se pronuncia DE LA MATA BARRANCO, N. J.: "El delito…" ob. cit. p. 164, cuando señala que "el Código […] insiste en que sólo se penalizan hechos graves, lo que trata de explicar reflejando dos veces el término grave, al describir el resultado producido, y ya antes, al referir la gravedad al borrado, daño, deterioro, alteración, supresión e inaccesibilidad".

[488] Este sería el caso típico de apagar el ordenador manteniendo cinco segundos apretado el botón de encendido (apagado a la fuerza), en lugar de apagarlo haciendo *click* en la opción de apagar sistema.

para, por ejemplo, suprimir datos, programas informáticos o documentos electrónicos que se puedan hallar contenidos en el interior de dicho soporte, con lo que la acción no sería típica por muy grave que fuese el resultado producido. En todo caso, tal requisito típico plantea un problema de indeterminación del tipo[489].

Como decíamos, el tipo añade a los elementos ya explicados que el resultado tenga una cierta entidad: "cuando el resultado producido sea grave" -también utiliza esta sistemática en su apartado segundo-. Para poder analizar oportunamente esta cuestión se tiene que conocer si nos encontramos ante un delito de resultado o de mera actividad. Los delitos de resultado son aquellos en los que para que se produzca la aparición completa del tipo, debe seguir a la acción del sujeto activo la producción de un resultado separado espaciotemporalmente de la misma, situación que no ocurre en los delitos de mera actividad[490]. La propia literalidad de los tipos analizados resuelve está cuestión, pues determina que debe producirse un resultado, que como estamos señalando ha de reputarse grave, para que se den las figuras reguladas[491].

El daño, además, debe ser probado y concretado[492]. A diferencia de la regulación de los daños clásicos en la que la determinación de la respuesta penal se configuraba en torno a un límite cuantificable y determinado de 400 euros, en el caso de los daños informáticos, ya en su regulación anterior, y también en la regulación actual se limita a considerar sólo acciones dignas de atención penal aquellas que dan lugar a un "resultado grave" sin indicar cuándo debe considerarse dicho resultado

[489] HUETE NOGUERAS, J.: "La reforma…" ob. cit. p. 3.

[490] MIR PUIG, S.: *Derecho…* ob. cit. pp. 221 y ss. y ZUGALDÍA ESPINAR, J. M.: *Fundamentos…* ob. cit. pp. 257 y ss.

[491] GONZÁLEZ RUS, J. J.: "El cracking y otros supuestos de sabotaje informático" en *Estudios Jurídicos. Ministerio Fiscal*, nº 2, 2003. El mismo autor en GONZÁLEZ RUS, Juan José: "Daños a través de Internet y denegación de servicios" en JORGE BARREIRO, A. (coord.): *Homenaje al profesor Dr. Gonzalo Rodríguez Mourullo*, Ed. Thomson Civitas, 1ª edición, Navarra, 2005, pp. 1472 y ss., GONZÁLEZ RUS, J. J.: "Los ilícitos en la red (I): hackers, crackers, cyberpunks, sniffers, denegación de servicio y otros comportamientos semejantes" en ROMEO CASABONA, C. M. (dir.): *El cibercrimen, nuevos retos jurídico-penales, nuevas respuestas político criminales*, Ed. Comares, Granada, 2006, pp. 248 y ss. y GONZÁLEZ RUS, J. J.: "Naturaleza y ámbito de aplicación del delito de daños en elementos informáticos" en DÍEZ RIPOLLÉS J. L., ROMEO CASABONA, C. M., GRACIA MARTÍN, L. e HIGUERA GUIMERÁ, J. F. (coords.): *La ciencia del Derecho penal ante el nuevo siglo. Libro homenaje al profesor doctor don José Cerezo Mir*, Ed. Tecnos, 1ª edición, Madrid, 2002), p. 248.

[492] MIRÓ LLINARES, F.: *Delitos…* ob. cit. p. 163. En referencia a la sentencia 234/2000 de la AP Granada sección 1ª de 6 de abril sobre daños sobre un bien inmueble.

grave a efectos típicos[493]. Ya hemos explicado en la introducción de este capítulo las dos vertientes doctrinales enfrentadas que sostenían la necesidad, o no, de aplicar el límite de 400 euros del tipo del artículo 263 CP también al antiguo 264.2 CP (y nuevo 264.1 CP). Aquellos que defendían la aplicación de dicho límite lo hacían por razones de seguridad jurídica y para sujetarse más estrictamente al principio de mínima lesividad[494]. Apoyando la interpretación opuesta, se encontraba aquel sector doctrinal que estimaba más ajustada a la literalidad del precepto la idea de que no era necesario ese límite, pues el legislador había decidido no incluirlo en el antiguo artículo 264.2 CP porque se configuraba como un tipo verdaderamente autónomo[495]. Lo que parece cierto, es que con la tipificación actual, en la cual se ha marcado una mayor separación entre los daños clásicos del artículo 263 CP, y los daños informáticos regulados en el artículo 264 CP, es incorrecto afirmar que el límite de los 400 euros rige en el caso de los daños informáticos. Sobre este asunto, en relación con la falta de daños del artículo 625 CP, volveremos en las páginas finales de este capítulo. Dicho esto, retomamos la cuestión de la concreción de la gravedad del daño para determinar su subsunción en el tipo o por el contrario su exclusión.

En primer lugar no podemos olvidar que nos encontramos en el ámbito de los delitos contra el patrimonio, por lo que se trata de valorar esa "gravedad" entendida siempre como un concepto económico. El daño producido debe poder ser cuantificable económicamente o, en su caso, será necesario poder hacer la equivalencia económica[496]. Lo cierto es que la doctrina no ha expuesto una tesis unitaria sobre cuándo debe considerarse grave el daño informático económicamente hablando[497] y se ha contentado con apuntar ciertos límites que ya hemos venido

[493] ANDRÉS DOMÍNGUEZ, A. C.: "Daños..." ob. cit. p. 294.

[494] DE LA MATA BARRANCO, N. J.: "El delito…" ob. cit. p. 164.

[495] DE LA MATA BARRANCO, N. J.: "El delito…" ob. cit. p. 165. En el mismo sentido MIRÓ LLINARES, F.: *Delitos…* ob. cit. pp. 163 y 164.

[496] MIRÓ LLINARES, F.: *Delitos…* ob. cit. p. 162.

[497] Sólo QUERALT JIMÉNEZ, J. J.: *Derecho…* ob. cit. p. 641, se ha aventurado a señalar como valor económica el perjuicio patrimonial sobre la víctima, calculado en torno al valor de la información y al trabajo (en tiempo y dinero) que ha supuesto para ella la creación o adquisición de esos datos, programas informáticos o documentos electrónicos. Cuestión que nos parece acertada, y en la línea de lo que se defenderá en la tercera parte de esta investigación, pero que, en cambio, supone una interpretación marcadamente extensiva de la que del daño patrimonial tradicional se hace en la actualidad.

avanzando. Estos son, que el daño tenga una valoración económica, para lo cual el tribunal deberá siempre tener la mirada puesta en el mercado[498], que los datos dañados tengan un valor funcional[499], que el menoscabo como disminución de la sustancia de los datos, programas informáticos o documentos electrónicos no será típico si no va acompañado de un perjuicio patrimonial a terceros[500], o que los gastos de reparación de un daño informático (que podría no ser típico en sí mismo por la falta de algún elemento) son perjuicios patrimoniales de carácter civil y que no integran el elemento objetivo del tipo[501]; en la misma línea se pronuncia la doctrina con respecto al lucro cesante[502]. Sin embargo, existen ya voces que no dudan en extender la idea de daño patrimonial, al menos en el ámbito de la delincuencia informática, a otros extremos tales como la relevancia social[503] del hecho o introduciendo nuevos conceptos económicos dentro del valor económico en el ámbito penal, como pueda ser el coste de recuperación del daño[504]. Sobre este y otros aspectos se realizará un amplio desarrollo en la tercera parte de esta investigación.

---

[498] MIRÓ LLINARES, F.: *Delitos*... ob. cit. p. 163, señala que "en la mayoría de los casos la valoración deberá hacerse conforme a los principios de la valoración del daño patrimonial, ponderándose las valoraciones predominantes en el mercado".

[499] MIRÓ LLINARES, F.: *Delitos*... ob. cit. p. 162, señala asumiendo la doctrina de los daños clásicos que "aquello que no tiene ningún valor no puede ser dañado en el sentido exigido. Al fin y al cabo daño en sentido económico es cualquier disminución de la utilidad de algo para un individuo".

[500] DE LA MATA BARRANCO, N. J.: "El delito…" ob. cit. p. 165.

[501] Así por ejemplo, cuando se dañan datos, programas informáticos o documentos electrónicos de muy poco o ningún valor económico con la infección por virus del sistema informático, pero la eliminación de ese virus supone un coste de varios cientos de euros, no se entenderá que el daño producido sea típico, pues la gravedad que exige el tipo objetivo se integra exclusivamente por valor económico del dato, programa o documento dañado, y no el coste (económico también) de la reparación. Véase el Auto de la AP Barcelona de 30 de octubre de 2000, que sigue la doctrina clásica del delito de daños, también en SANTA CECILIA GARCÍA, F.: *Delito*… ob. cit. p. 272.

[502] MIRÓ LLINARES, F.: *Delitos*... ob. cit. p. 163, expresa "en cuanto a la posibilidad de tener en cuenta el lucro cesante a los efectos del daño en sentido penal […] el mismo se puede tener en cuenta a la hora de la responsabilidad civil *ex delicto* pero no para la determinación de la existencia del tipo objetivo de daños".

[503] Así, RAGUÉS I VALLES, R. y ROBLES PLANAS, R.: "La reforma…" ob. cit. p. 374, señala que aunque exista afectación patrimonial, y ésta pueda ser un buen indicio, la "exigencia de gravedad de la conducta hace referencia a la valoración jurídico-social de la misma".

[504] MATELLANES RODRÍGUEZ, N.: "Algunas notas sobre las formas de delincuencia informática en el Código Penal" en DIEGO, DÍAZ-SANTOS M. R. y SÁNCHEZ LÓPEZ, V. (coords.): *Hacia un Derecho penal sin fronteras*, Ed. Colex, 1ª edición, Madrid, 2000, p. 143, para justificar la aparición del daño grave se remite a señalar que "no es necesario que el daño económico sea un daño patrimonial *strictu sensu*" para luego afirmar que "toda conducta de sabotaje informático conlleva un perjuicio

Para finalizar este apartado se nos presenta la cuestión referida a la de aquellos datos que tienen un valor personal importante para los perjudicados, pero que no es posible traducirlo claramente a la esfera económica porque en realidad, valor patrimonial como tal no poseen. ¿Podemos afirmar entonces que la conducta sea atípica? La respuesta de la doctrina parece posicionarse en el sentido de descartar que este tipo de objetos, en este caso datos, programas y especialmente documentos electrónicos (que suelen ser fotos, videos y otros documentos electrónicos de esta naturaleza) tengan un valor económico real, y por tanto la protección de los mismos no puede realizarse a través del delito de daños[505]. Aunque es cierto que también se posiciona algún autor en el extremo contrario, al considerar que estos bienes de carácter personal o moral, aunque no pueda traducirse dicho valor en un concepto económico, deben ser protegidos en los casos de especial gravedad[506]. Contra esta segunda interpretación, tal y como está ubicado el tipo penal, cabe interponer algunos reproches. Es muy loable que se pretendan castigar ciertas conductas realizadas en contra de aquellos sujetos para quienes un objeto pueda tener un valor sentimental -o moral-, y la realidad es que ya se están protegiendo. La reparación civil[507] -aún sustanciada en el proceso penal[508]- es la adecuada en este ámbito en

económico muy elevado, pues mediante él al titular o usuario de ordenador se le priva de su sistema de gestión (contabilidad, administración, cartera de clientes), o incluso, de planificación y organización del trabajo."

[505] DE LA MATA BARRANCO, N. J.: "El delito…" ob. cit. p. 165, expresa que "lo que sí está claro […] si no se produce afección patrimonial alguna, la conducta analizada habrá de considerarse atípica, por más que pueda ser insatisfactorio entender impunes daños que simplemente afectan a un desenvolvimiento personal, no patrimonial, por ejemplo en supuestos como el de una tesis doctoral borrada en todas sus copias por un virus". No obstante, aun estando de acuerdo en la posición general mantenida, precisamente el ejemplo propuesto por el autor referido a una tesis doctoral, no parece el más adecuado, pues la realización y posterior destrucción de dicha tesis no creemos que afecte exclusivamente a lo que el autor denomina "desenvolvimiento personal".

[506] Así lo defiende MIRÓ LLINARES, F.: *Delitos…* ob. cit. p. 162, al señalar que "el daño en estos bienes, cuando no tengan ningún valor patrimonial, sería protegible por el CP art. 264 en los casos en los que se tratase de un resultado grave".

[507] NÚÑEZ FERNÁNDEZ, J.: "Otras consecuencias del delito: la responsabilidad civil *ex delicto*, las costas procesales y las consecuencias accesorias" en GIL GIL, A., LACRUZ LÓPEZ, J, M., MELENDO PARDOS, M. y NÚÑEZ FERNÁNDEZ, J.: *Curso de Derecho penal. Parte General*, Ed. Dykinson, Madrid, 2011, pp. 950 y ss.

[508] DE LA OLIVA SANTOS, A.; ARAGONESES MARTÍNEZ, S.; HINOJOSA SEGOVIA, R.; MUERZA ESPARZA, J. y TOMÉ GARCÍA, J. A.: *Derecho Procesal Penal*, Ed. Editorial Universitaria Ramón Areces. 8ª edición, Madrid, 2007, pp. 244 y 245, "la acción civil que cabe ejercitar en el proceso penal para la restitución de la cosa, la reparación del daño y la indemnización de perjuicios (y otros

consonancia con el bien jurídico que protege la figura de daños en nuestro ordenamiento penal[509]. Pero es que además, siguiendo las principios clásicos de menor lesividad, taxatividad o mínima intervención del Derecho penal, aceptar estos daños como típicamente relevantes daría lugar a una inseguridad jurídica que el Derecho penal no debe permitir, pues su configuración actual deberá referirse siempre a daños concretos, o que se puedan concretar con objetividad económica, situación que deja de existir cuando debemos entrar a valorar el valor personal de esos datos y traducirlo a la esfera económica, más si cabe cuando existen otras vías para reclamar ese daño "moral" producido[510]. Habilitar el reproche penal en este sentido sería vaciar de contenido en gran medida la reclamación civil por daños en todos estos ámbitos. Manteniendo, pues, la idea de que los datos personales sin valor económico no están protegidos por la regulación tal y como está ubicado el precepto, lo que sí es cierto y causará mayores problemas será diferenciar ciertos datos respecto de los que no pueda delimitarse de manera exacta si tienen un carácter personal o por el contrario tienen un valor económico real y cuantificable[511]. De la misma manera que se expresaba antes, estas cuestiones deberán ser valoradas en cada caso por los tribunales.

Por último, y será tratado en la tercera parte de esta investigación, cabe preguntarse lo que ocurriría de extraer el tipo penal del artículo 264.1 CP -en realidad

---

contenidos, en casos especiales) no deriva del delito ni de la falta criminal, sino de actos u omisiones ilícitos -pero no necesariamente delictivos- que produzcan injustas consecuencias negativas o daños y perjuicios".

[509] ANDRÉS DOMÍNGUEZ, A.C.: *El Delito*... ob. cit. p. 122. "el valor económico constituye un elemento típico del delito de daños. La cosa corporal y ajena ha de ser económicamente valorable, valor que se encuentra insito en la misma. […] Consecuentemente los bienes privados de valor de cambio pero poseedores de gran valor afectivo (bienes de valor afectivo) no pueden ser objeto material de daños". También SANTA CECILIA GARCÍA, F.: *Delito*… ob. cit. pp. 243 y ss.

[510] Está situación ya se aventuraba, incluso antes de que se tipificaran los delitos de daños informáticos en el Código de 1995 en MIR PUIG, S. *Delincuencia Informática*, Ed. PPU, 1ª edición, Barcelona, 1992, pp. 172 y ss., al señalar precisamente que la valoración económica de dichos objetos no podía calcularse. En cambio, sí podía calcularse el perjuicio (más general) causado con su destrucción, lo que llevaría, en caso de quererse castigar tales conductas, a una reinterpretación del daño penal.

[511] Puede pensarse por ejemplo en el caso de un fotógrafo que realiza las fotos para luego venderlas a una revista, de tal forma que aunque es complicado determinar el valor de las fotos, más si cabe cuando ya no pueden ser vistas por perito o experto que las valore, es indudable que no tenían un valor puramente personal, sino que de ellas se presumía un valor económico real. El mismo ejemplo podría suceder con el autor de una novela, un diseñador de páginas web, etc.

excluirlo de los delitos de daños en particular, o incluso de los delitos patrimoniales-. A nuestro juicio, uno de los problemas fundamentales que suscita la inclusión de los daños informáticos como tipos de daños patrimoniales queda manifestado a la hora de interpretar la gravedad del daño con el *corsé* impuesto por doctrina y jurisprudencia, que exige su interpretación acorde a los daños tradicionales y que, obviamente, no estaba pensada para el caso de objetos inmateriales. Un posible cambio sistemático de estos tipos penales abriría las puertas a efectuar un nuevo estudio y determinación -doctrinal y jurisprudencial- de los conceptos señalados que, probablemente, construirían una interpretación del tipo penal más racional o, al menos, que suscitase menos incógnitas.

b.1.8. La ajenidad y la falta de autorización.

El tipo penal exige, como elemento del tipo, que el objeto sobre el que recae la acción del daño sea ajeno al autor, es decir, el sujeto activo nunca lo será si efectúa las acciones típicas sobre datos, programas informáticos o documentos electrónicos propios, si bien para entender cuando éstos son ajenos o, por el contrario, propios, sería conveniente acudir a la regulación civil oportuna[512], aunque también cabría preguntarse si es válida la interpretación que de éste concepto se realiza en otros tipos penales[513].

El otro aspecto que analizamos en este punto es el referido a la falta de autorización, que no debe ser entendida sino como el consentimiento clásico[514]. Utilizar el concepto de autorización en lugar del de consentimiento es fruto de la traducción de la Decisión Marco, que probablemente no haya sido la más adecuada, pues la figura clásica de nuestro Derecho es el consentimiento y no la autorización,

[512] DE LA MATA BARRANCO, N. J.: "El Delito…" ob. cit. p. 168.

[513] Por ejemplo el tratamiento que de la ajenidad se da en el caso del hurto, también configurado como un delito patrimonial, MUÑOZ CONDE, F.: *Derecho…* ob. cit. p. 381 y QUERALT JIMÉNEZ, J. J.: *Derecho penal español. Parte especial*, Ed. Atelier, 6ª edición, Barcelona, 2010, p. 642. Todo ello partiendo de que, en lo relativo a la propiedad de los documentos y programas informáticos, puede plantearse la situación en la que un programador que ha realizado un programa informático, del que será propietario aun cuando un tercero lo haya adquirido para el uso, haya implementado una subrutina oculta, de forma similar a una bomba lógica, que cuando él decide daña todas las copias de su *software*. No parecería lógico pensar que la figura sea atípica por falta del requisito de la ajenidad, lo que llevaría a diferenciar entre la propiedad intelectual sobre el *software* y la propiedad para uso y explotación del tercero adquirente.

[514] FLORES PRADA, I.: *Criminalidad*… ob. cit. p. 165.

aunque puedan entenderse en el caso presente como equivalentes[515]. Pero dejando al margen estas cuestiones, parece lógico que si el daño sólo es típico cuando se realiza sobre un objeto ajeno, además tenga que contar con la oposición del perjudicado.

El consentimiento se configura en el ámbito penal como la facultad dispositiva que un titular del bien jurídico protegido tiene sobre el mismo[516]. A este respecto no podemos obviar que la discusión sobre el consentimiento como figura dentro del Derecho penal ha deparado gran cantidad de comentarios en la doctrina. Desde las primeras expresiones romanas que pretendían excluir la responsabilidad penal en los casos en que mediaba el consentimiento del ofendido: *nulla iniuria est, quae in volentem fiat* ("lo que se realiza con la voluntad del lesionado, no constituye injusto"), transformada posteriormente en la máxima *volenti non fit iniuria* ("la voluntad no hace injusto"), hasta la actual concepción de esta compleja figura se han ido sucediendo muy variadas visiones dogmáticas[517]. En la actualidad, en la doctrina alemana, se contraponen dos figuras concretas dentro de lo que podemos entender como el consentimiento en sentido amplio: el acuerdo y el consentimiento en sentido estricto; siendo las consecuencias de uno u otro diferentes[518]. Mientras que el acuerdo excluye la tipicidad del hecho, el consentimiento en sentido estricto podrá suponer sólo la exclusión de antijuridicidad (justificación) de la acción típica[519]. La doctrina alemana entiende por acuerdo aquellas situaciones en las que la no existencia de oposición a la vulneración del bien por parte del sujeto pasivo implica la falta de tipicidad, pues en realidad no se ha llegado a vulnerar el bien jurídico protegido. Por el contrario en los casos de consentimiento en sentido estricto, si se está poniendo en juego el bien jurídico protegido, de hecho, se habrá producido la lesión de dicho bien, pero el consentimiento del sujeto pasivo justificaría dicho

[515] La Decisión Marco 2005/222/JAI de 24 de febrero, en su artículo 1 define que debe entenderse por falta de autorización "el acceso o la intromisión no autorizados por el propietario o titular de otro tipo de derecho sobre el sistema o parte del mismo o no permitidos por la legislación nacional". Desde luego una definición manifiestamente mejorable, en primer lugar por incluir en la definición la palabra definida, y en segundo lugar porque termina por remitir al derecho nacional en cada caso, siendo en nuestro caso la figura del consentimiento la adecuada.

[516] MUÑOZ CONDE, F. y GARCÍA ARÁN, M.: *Derecho Penal…* ob. cit. pp. 343 y ss.

[517] Un visión más amplia se puede observar en ROXIN, C.: *Derecho…* ob. cit. pp. 511.

[518] ROXIN, C.: *Derecho…* ob. cit. p. 512.

[519] Con reservas MIR PUIG, S.: *Derecho…* ob. cit. pp. 511 y 512.

daño[520]. Esta concepción del sistema alemán es igual a la que la doctrina ha seguido en el Derecho español, si bien en el nuestro ambos son denominados indistintamente como consentimiento.

Lo cierto es que nuestro Código penal no aborda las cuestiones relativas al consentimiento[521], si bien no parece haber dudas de que el propio Código penal utiliza la figura con dos fines diferentes. Por un lado, parece utilizar el consentimiento como elemento típico de algunos delitos[522]; y por otro lado, se refiere al mismo para ubicarlo como una suerte de atenuante en otra serie de delitos[523]. Es decir, que podría actuar tanto como causa de atipicidad como causa de justificación. En todo caso, la visión dogmática alemana antes apuntada no se corresponde con el tratamiento jurídico que el Código penal otorga al consentimiento, lo que se traduce en el dispar tratamiento del mismo en nuestra doctrina[524].

Volviendo de nuevo a los daños informáticos, parece que la redacción del tipo considera la falta de consentimiento (de autorización) como un elemento típico, y por tanto, actuando con el consentimiento del propietario de los datos, programas informáticos o documentos electrónicos, la conducta sería atípica. Pero no podemos obviar la dogmática alemana antes explicada, según la cual debemos diferenciar

---

[520] MIR PUIG, S.: *Derecho…* ob. cit. pp. 509 y ss.

[521] Aunque algunos autores afirmen que se trata inequívocamente de una causa de justificación más del artículo 20 CP, véase MUÑOZ CONDE, F. y GARCÍA ARÁN, M.: *Derecho Penal…* ob. cit. p. 343, que señalan que "el consentimiento es la única causa de justificación no citada expresamente entra las eximentes del art. 20." Otra parte de la doctrina, en cambio, se posiciona en contra de esta visión, véase QUINTERO OLIVARES G.: *Parte*… ob. cit. p. 502, "es notorio que en el Derecho penal positivo español no existe una circunstancia eximente de consentimiento". Lo cierto es que el único tratamiento sobre las consecuencias del mismo que realiza nuestro Código penal se ubica en el artículo 155 relativo a las lesiones.

[522] Expresamente, por ejemplo, en el delito de allanamiento de morada (art. 202 CP) o el hurto (art. 234 CP), aunque MIR PUIG, S.: *Derecho…* ob. cit. p. 510, entiende su aparición de forma tácita en otros delitos como los de detenciones ilegales (art. 163 CP), en el cual, el consentimiento del detenido elimina la ilegalidad de la detención.

[523] Expresamente lo hace en el art. 155 CP en el caso de las lesiones o en el 145.1 CP relativo al que practica un aborto con consentimiento de la embarazada.

[524] QUINTERO OLIVARES G.: *Parte…* ob. cit. p. 501, "sucede que el tema del consentimiento no ha sido casi nunca, al menos en la doctrina española, objeto de tratamiento global […] Es fácil apreciar en los programas de Parte General la inclusión del consentimiento unas veces en las causas de ausencia de acción (típica) y otras entre las causas de justificación, aun, cuando es sabido, no figure en el catálogo del artículo 20 CP una circunstancia eximente de tal clase".

entre que se haya producido la lesión del bien jurídico protegido con consentimiento del titular del mismo -consentimiento en sentido estricto- de aquella situación en la que el mero consentimiento del titular hace desaparecer la protección penal, pues la conducta no puede subsumirse como típica por falta de un elemento esencial (acuerdo). Según esta visión, los daños informáticos, cuyo sujeto pasivo es determinado, siendo el bien jurídico protegido el patrimonio particular (en concreto el valor económico de los datos, programas informáticos o documentos electrónicos dañados) aun cuando se produzcan con consentimiento, podría entenderse que la acción habrá lesionado el bien jurídico protegido, pues el valor habrá sido afectado, y por tanto, dicho consentimiento podría actuar como causa de justificación, pero no convertirá la figura en atípica[525].

Sin embargo, nos parece más correcto concluir que el hecho de que en los delitos del artículo 264 CP la autorización aparezca como un elemento más dentro del tipo -si se admite esta equivalencia con el concepto de consentimiento-, de existir, devendría en la falta de concurrencia de uno de los elementos del tipo penal, por lo que según nuestro criterio ello supondrá, para el caso concreto de los delitos del artículo 264 CP, una causa de atipicidad, y no una causa de justificación.

Por último, no debemos obviar la figura del riesgo permitido asociado al consentimiento[526], pues en este último caso, el sujeto pasivo en los daños informáticos, puede aceptar el riesgo que supone para sus datos, programas informáticos, o documentos electrónicos las operaciones que un tercero va a realizar sobre ellos, conociendo que de éstas se puede derivar un daño que, en este caso, podría resultar típico y, por tanto, el consentimiento prestado para la realización de dichas operaciones de riesgo, atendiendo a las circunstancias concretas del caso, podría actuar de nuevo como causa de exención de responsabilidad penal por falta de tipicidad. A ello nos referiremos cuando estudiemos la posible aparición de supuestos de omisión en el tipo penal.

---

[525] ROXIN, C.: *Derecho…* ob. cit. p. 512, señala que "el consentimiento en sentido estricto, cuando es prestado por el portador del bien jurídico, sólo tendrá efecto de justificación, pero no el de excluir la realización del tipo. Los ejemplos fundamentales los proporcionan los tipos de daños y las lesiones".

[526] QUINTERO OLIVARES G.: *Parte…* ob. cit. p. 509, "el riesgo permitido es para muchos autores un criterio determinante de la desaparición de la tipicidad".

b.2. Elementos del artículo 264.2 CP.

El apartado segundo del artículo 264 CP es coincidente con el primero en cuanto se refiere, en similares términos, a quien "por cualquier medio, sin estar autorizado, y de manera grave" cometa una serie de actos alternativos consistentes en: "obstaculizar o interrumpir el funcionamiento de un sistema informático ajeno", pero siendo necesariamente a través de una de las siguientes técnicas: "introduciendo, transmitiendo, dañando, borrando, deteriorando, alterando, suprimiendo o haciendo inaccesibles datos informáticos". También, al igual que la conducta del primer apartado, establece que "el resultado producido sea [fuera] grave" como un elemento imprescindible.

b.2.1. El uso de las fórmulas "por cualquier medio", "sin estar autorizado", "de manera grave" y con un "resultado producido grave" y la de "ajenidad" en el tipo del artículo 264.2 CP.

Por lo que respecta a la mayor parte de los elementos que se estructuran en este segundo apartado del artículo 264 CP podemos aceptar, con alguna salvedad, la misma interpretación que hemos dado para los elementos del apartado anterior.

En primer lugar, creemos que es necesario puntualizar el hecho de que la expresión utilizada de "cualquier medio" en este caso es equivocada y conduce a error. No sólo no es "cualquier medio", sino que únicamente puede serlo aquel que sea idóneo, como explicamos en la interpretación realizada para acomodar el término "de manera grave". Esta vez, además, ese "cualquier medio" queda considerablemente reducido por las conductas a través de las cuales el propio artículo 264.2 CP limita la obstaculización o la interrupción, que sólo podrá ser introduciendo, transmitiendo, dañando, borrando, deteriorando, alterando, suprimiendo o haciendo inaccesibles datos informáticos.

Esta aparente contradicción nos hace preguntarnos algunos extremos; por ejemplo, si la obstaculización o interrupción de sistemas informáticos que puede llevarse a cabo por la destrucción física del propio sistema tendría cabida en el tipo o no, es decir, si la destrucción física del objeto material se entiende como medio penalmente válido para conseguir obstaculizarlo o interrumpirlo. Creemos que con la

actual redacción, a pesar de la fórmula "por cualquier medio" y a diferencia del caso del tipo del artículo 264.1 CP, estamos ante un delito de medios determinados, de forma que la única manera de producir la obstaculización o interrupción será introduciendo, transmitiendo, dañando, borrando, deteriorando, alterando, suprimiendo o haciendo inaccesibles datos informáticos. En realidad, lo que se castiga principalmente -pero no únicamente- en este precepto es al que cometiendo las acciones del artículo 264.1 CP, además, interrumpa u obstaculice un sistema informático en su totalidad, siempre que se cumplan los requisitos de doble gravedad. Es decir, sanciona específicamente un resultado del apartado anterior. Visto de esta manera y remitiéndonos a lo ya apuntado en el análisis de artículo 264.1 CP en el que se aceptaba como un medio posible para producir el daño sobre datos, programas informáticos o documentos electrónicos el ataque físico al *hardware* donde se contenía ese dato, podemos concluir que cabe la posibilidad de que la interrupción u obstaculización se lleven a cabo por medio de un ataque físico al sistema informático, siempre que este ataque dañe esos datos, programas o documentos, y esos daños a la vez produzcan la interrupción u obstaculización del sistema informático en general.

Sin embargo, aun aceptando esta tesis no podemos dejar de afirmar que es un delito que sólo se puede cometer a través de una de las conductas tasadas por el propio tipo, esto es, o bien introduciendo o transmitiendo datos, o bien a través de una de las acciones del apartado primero. Esto es así incluso aun cuando el propio artículo establezca que puede ser "por cualquier medio".

Lo cierto es que al dar entrada a la interpretación que se hace de las acciones del apartado primero en este segundo apartado, parece poco probable que puedan existir más modos por los que poder cometer las acciones de interrupción y obstaculización, de tal manera que quedan cubiertos todos los medios[527], como bien quiere establecer el legislador. Otra cuestión será que la redacción de este artículo 264.2 CP sea la más adecuada, extremo que será debatido más adelante.

[527] Es la tesis seguida por MIRÓ LLINARES, F.: *Delitos*... ob. cit. p. 165, que señala con acierto que "puede decirse que están todas, puesto que los datos en informática o se introducen, o se transmiten, o se dañan, o se borran, o se deterioran, o se alteran, o se hacen inaccesibles."

Respecto al requerimiento de doble gravedad que también utiliza el legislador en este segundo apartado, la doctrina sigue considerando que se trata de una imposición redundante o innecesaria[528]. Al igual que en el caso anterior, creemos que es un error esta manera de tratar el sentido de la doble exigencia de gravedad en el tipo. Son dos esferas diferenciadas, la que exige que el resultado sea grave (con los problemas de interpretación que vimos que conlleva) y la exigencia de que el modo de conducta empleado sea grave, esto es, que sea el idóneo para producir el resultado grave, reduciendo las posibilidades de la ya de por si limitada expresión "por cualquier medio" que hemos analizado en este segundo apartado.

Las cuestiones relativas a la autorización y la ajenidad a que nos hemos referido respecto al primer apartado, se reproducen en este segundo, sin que aparentemente se pueda añadir nada a lo ya expuesto. Por un lado, la interrupción u obstaculización del sistema debe operarse sobre un sistema ajeno y además no debe estar consentido por el legítimo propietario del mismo (entendido en sentido amplio). Como cuestión casi anecdótica cabe mencionar que el legislador haya decidido utilizar dos construcciones lingüísticas diferentes en cada tipo: mientras que en el primero utiliza la expresión "sin autorización", en el segundo utiliza "sin estar autorizado". No creemos necesario profundizar más en este cambio, si bien sumado a otras cuestiones que hemos analizado -más otras a que aludiremos en las siguientes páginas- nos hacen plantearnos por la idoneidad de las elecciones tomadas en sede legislativa en la regulación de estos tipos penales.

b.2.2. Las acciones de interrumpir y de obstaculizar.

Las acciones típicas de este apartado segundo del artículo 264 CP son las de interrumpir y obstaculizar un sistema informático, conductas cuyo significado y extensión no ha sido debidamente analizado por la doctrina española, en parte debido a que son dos acciones de reciente aparición en nuestro ordenamiento penal, que han venido a responder como el resto de la regulación en esta materia a los imperativos de las instituciones europeas a través de la Decisión Marco 2005/222/JAI de 24 de febrero.

[528] MIRÓ LLINARES, F.: *Delitos…* ob. cit. p. 165, vuelve a definir esta imposición de doble gravedad como "error de duplicar la exigencia de gravedad".

Siguiendo la definición que la Real Academia de la Lengua da al verbo interrumpir, conforme a la cual consiste en "cortar la continuidad de algo en el lugar o en el tiempo", no podemos delimitar correctamente qué debe entenderse por interrumpir en el ámbito informático. En principio, lo que debemos valorar es aquello que el legislador ha pretendido proteger sancionando estas conductas. Parece que si lo que se sanciona es cortar la continuidad de un sistema informático en realidad se está castigando inutilizar durante un periodo de tiempo, tanto definida como indefinidamente. Al igual que las acciones anteriores, tiene que producir un resultado grave desde el punto de vista del perjuicio económico, por lo que un ataque que provoque una interrupción mínima difícilmente sería considerado típico, siempre que esos ataques no se repitiesen en el tiempo. Siendo el caso de que se produjesen interrupciones mínimas pero repetidas en el tiempo, cabría preguntarse si nos encontraríamos entonces ante una continuidad delictiva contemplada en el artículo 74.2 CP o, como parece más correcto, deberíamos subsumir la conducta en la acción de obstaculizar que analizamos a continuación.

De la misma forma que hicimos con la acción de interrumpir, podemos observar que la Real Academia de la Lengua define obstaculizar como "impedir o dificultar la consecución de un propósito". Lo que en este caso se sanciona no es que el sistema informático quede inutilizado en sus funciones, sino un grado algo inferior, aunque de consecuencias igualmente reprochables para el legislador. La obstrucción debe entenderse como la dificultad de utilizar ese sistema informático conforme a su funcionalidad habitual. Las posibilidades de obstaculización de un sistema informático tendrán un carácter menos grave que la interrupción en general, aunque, como ya avanzamos, tal acción puede resultar en ocasiones igual de grave que la interrupción, por cuanto existe un punto en que la obstaculización de un sistema puede ser de tal magnitud que equivalga, fácticamente, a la interrupción del mismo.

Ambas conductas tienen en común que no dañan en el sentido estricto de la palabra los elementos lógicos, o por lo menos no necesariamente[529], y se identifican normalmente con los ataques que tienen por objeto inutilizar o bloquear durante un

[529] MIRÓ LLINARES, F.: *Delitos…* ob. cit. p. 164.

periodo de tiempo los servidores de páginas webs o servidores de empresa. Estas acciones suscitaban problemas conforme la redacción anterior a la reforma, lo que produjo la situación de que los tribunales desestimaran procesos con este objeto por cuestiones de atipicidad penal[530]. El auto de la AP de Madrid 229/2004 de 21 de mayo, establecía entre otros motivos que "es preciso atender a la apreciación de la gravedad y antijuridicidad de la conducta, considerando el conjunto de circunstancias concurrentes, en aplicación del principio de intervención mínima que excluye la sanción penal en los supuestos en que el ordenamiento jurídico provea de medios o instrumentos adecuados para resolver el conflicto, y ello porque el derecho punitivo cumple una función de carácter subsidiario y consiste en la última ratio" [531]. Lo que no deja de resultar cuando menos curioso, es que estas actuaciones, que no encontraban acomodo en la regulación penal anterior por suponer en general conductas de menor gravedad que las reguladas (según se desprende de la escasa jurisprudencia), tengan ahora, con una regulación expresa, una penalidad mayor que la de los daños informáticos del 264.1 CP que ya se encontraban tipificados. Es cierto también que se pueden encontrar en la realidad jurisdiccional sentencias en las que se reconoce como tal la figura de obstaculizar e interrumpir como subsumibles en el antiguo 264.2 del Código penal. Este es el caso de la sentencia dictada por el Juzgado de lo Penal número de 2 de Lleida[532] en el que no se duda en señalar en los hechos probados que "el acusado […] decidió vengarse realizando ataques de denegación de servicio distribuida (DDoS), consistente en múltiples ataques simultáneos y masivos en el tiempo que colapsaron las líneas impidiendo durante amplios lapsos temporales toda actividad" para a continuación condenarlo por un delito del antiguo artículo 264.2 del Código penal.

[530] GONZÁLEZ RUS, J. J.: "El cracking…" ob. cit. p. 245, señala que un ataque informático de estas características, con la regulación del antiguo 264.2 CP no podría ser nunca acción típica sin una extensión excesiva de la interpretación del precepto.

[531] Auto de la AP de Madrid 229/2004 de 21 de mayo, que entiende que la acción de obstaculizar el funcionamiento de un servidor de comunicaciones sin "dañar" datos, programas informáticos o documentos electrónicos no podía sino resolverse en la vía civil por el perjuicio causado, pero no en sede penal donde la acción no podía ser típica en base a los elementos del artículo 264.2 CP vigente en ese momento.

[532] SJP número 2 de Lleida 33/2006 de 7 de febrero.

Lo que queda claro, pues, es que era necesaria la inclusión en la reforma de los daños informáticos de una fórmula que aclarase estos supuestos, para evitar así la inseguridad jurídica producida por la tipicidad (o no) de estos ataques consistentes en la obstaculización o interrupción de sistemas.

b.2.3. Los modos de interrumpir y de obstaculizar.

Como ya hemos señalado con anterioridad, aunque el apartado segundo del artículo 264 CP establece que "cualquier medio" es válido para cometer las acciones que acabamos de analizar, lo cierto es que el propio artículo se autolimita en este sentido, al establecer que las acciones típicas lo serán cuando se llevan a cabo introduciendo o transmitiendo datos o llevando a cabo alguna de las acciones típicas del apartado primero, siempre todas ellas sobre datos informáticos. Así, en este apartado vamos a analizar las dos primeras conductas, que son las novedosas, finalizando con una mención de los modos coincidentes con las acciones del artículo 264.1 CP.

a) Introducir o transmitir datos informáticos

En primer lugar nos referiremos a la cuestión de "introducir" sobre la que la doctrina tampoco se ha manifestado. La RAE lo define como "meter o hacer entrar algo en otra cosa". Visto de este modo, en el campo informático no puede separarse especialmente el significado de la figura común, si acaso concretarse a través de la descripción del tipo en que se expresa que lo que se introduce son datos informáticos en un sistema informático. La cuestión que se puede plantear es la referida a si introducir datos en un sistema informático puede subsumirse en una acción más general, como pueda ser la de alterar datos en un sistema informático. La respuesta parece afirmativa, pues alterar los datos de un sistema informático pasa por tres posibilidades: añadirlos, modificar los que existan, o quitarlos, de tal forma que como ya vimos en algunas acciones del artículo 264.1 CP se reproduce la redundancia a la que se ha acostumbrado el legislador en estos casos. Aunque la cuestión no afecta directamente a la explicación del tipo, parece necesario anotarla.

La conducta de transmitir datos, por el contrario, sí es una conducta nueva cuya inexistencia convertía en atípicos hechos que ya se estaban produciendo en la

realidad. Viene a colmar la necesidad de sancionar conductas que no afectan a la integridad de los datos informáticos, pero que igualmente puede producir que un sistema informático sufra una interrupción o una obstaculización. Es el caso clásico de los ataques de denegación de servicios, o DDoS[533]. En estos supuestos, el atacante no realiza ninguna acción sospechosa sobre los sistemas informáticos que pretende atacar, simplemente satura su capacidad transmitiendo peticiones al servidor que va haciéndolo responder cada vez de manera más lenta hasta que finalmente no es capaz de procesarlas y se ve bloqueado. En principio, la transmisión de datos informáticos no afecta a la integridad del sistema informático, pues es la práctica habitual de comunicación entre sistemas, lo que afecta es una cantidad sobredimensionada de estas peticiones al sistema. Es a través de este método como mejor se puede observar como las conductas del artículo 264.2 CP no sólo protegen la integridad de los datos o sistemas informáticos, sino que se va un poco más allá tratando de tutelar también el normal funcionamiento de los mismos, se afecte o no a la sustancia del objeto material. En un sentido estricto, no se está dañando nada, lo que no implica que tal acción no merezca un reproche penal, pero sí que quizá, su ubicación en el ámbito de los delitos de daños no sea la más adecuada para la tipificación de este tipo de conductas.

b) Dañar, borrar, deteriorar, alterar, suprimir o hacer inaccesibles datos informáticos

Por lo que respecta a las conductas que son coincidentes con las acciones del apartado primero no parece que se pueda añadir nada en particular respecto de lo ya expresado sobre cada una de ellas. En principio la interpretación de los términos debe ser la misma, con la diferencia de que aquí la sola conducta no supone el hecho típico, sino que debe producirse un resultado concreto, esto es la interrupción u obstaculización de un sistema informático (que además tiene que ser grave). Podemos afirmar que lo que se castiga en este apartado segundo es que las acciones

[533] Siglas en inglés de *Distributed Denial of Service*. Es un ataque a un sistema de red que provoca que un servicio sea inaccesible a los usuarios que hacen uso de él. El problema principal que causa este tipo de ataques es la pérdida de conectividad de la red por el consumo del ancho de banda de la red víctima, provocando así que ese servicio esté caído hasta que se consigue controlar el ataque.

del primer apartado no causen cualquier daño grave, sino en concreto el de interrumpir u obstaculizar, que se considera contiene un mayor desvalor, y por ello se castiga con mayor penalidad.

b.3. Modalidades comisivas.

Por lo que respecta a modalidad comisiva de estos delitos, atendiendo a la forma que ha elegido el legislador de regular el tipo, está pensando fundamentalmente en una acción positiva por parte del sujeto activo, que es el que inicia la serie de acontecimientos que van a determinar la producción de un resultado. Pero ello no indica que no se deban hacer algunas precisiones sobre la modalidad omisiva.

Se debe descartar la figura de la omisión pura por cuanto no se tipifica de forma expresa ninguna modalidad omisiva en el Código penal[534]. Sin embargo, sí procede que nos preguntemos si cabe la posibilidad de la comisión por omisión[535]. En principio, tal forma de comisión, regulada con carácter general en el artículo 11 del Código penal, atendiendo a su ubicación sistemática en el Libro I del Código, puede ser aplicada a todos los delitos de resultado[536]. La cuestión es si la realidad propia de estos delitos permite la efectiva realización de los tipos por omisión. Para ello deberemos verificar si se dan las condiciones que doctrina y jurisprudencia han construido a través del citado artículo 11 del Código penal[537].

---

[534] Según la bipartición que recoge MIR PUIG, S.: *Derecho*... ob. cit. pp. 313 y ss., se distingue que entre los delitos de omisión prevista como tal por la ley y los de omisión no descrita expresamente por la redacción legal. Mientras que en los primeros cabe la figura de la omisión pura, en los segundos (que es el caso en el que nos encontramos) sólo cabe la comisión por omisión. También OCTAVIO DE TOLEDO Y UBIETO, E. y HUERTA TOCILDO, S.: *Derecho*… ob. cit. pp. 560 y ss.

[535] SANTA CECILIA GARCÍA, F.: *Delito*… ob. cit. pp. 237 y ss., señala, aun refiriéndose a los daños tradicionales, que "la configuración del delito de daños como de resultado hace perfectamente posible la comisión por omisión". Conclusión que cabe extender a los daños informáticos. Para un estudio completo véase DOPICO GÓMEZ-ALLER, J.: *Omisión e injerencia en Derecho Penal*, Ed. Tirant lo Blanch, 1ª edición, Valencia, 2006.

[536] HUERTA TOCILDO, S.: *Principales novedades de los delitos de omisión en el Código penal de* 1995, Ed. Tirant lo Blanch, 1ª edición, Valencia, 1997, pp. 20 y ss. MUÑOZ CONDE, F. y GARCÍA ARÁN, M.: *Derecho*... ob. cit. p. 243. "El delito realizado en comisión por omisión es un delito de resultado".

[537] Artículo 11 CP: "Los delitos o faltas que consistan en la producción de un resultado sólo se entenderán cometidos por omisión cuando la no evitación del mismo, al infringir un especial deber

Vayamos por partes. El tipo del artículo 264.1 CP debería castigar, entonces, que el daño sobre los datos, programas informáticos o documentos electrónicos se produzca porque un sujeto no haya evitado el resultado teniendo la capacidad de hacerlo cuando tenía una posición de garante del bien jurídico protegido y se le pueda imputar objetivamente el resultado[538]. La pregunta es entonces fácil, ¿quién puede ser garante respecto del delito de daños del apartado primero? En principio, como delito común, al igual que para las modalidades activas, cualquier persona puede situarse en posición de garante. Pero hagamos algunas reflexiones al respecto.

Aunque la doctrina tiende a dividir en dos grandes grupos los posibles garantes, el primero referido a la función de protección del bien jurídico protegido, y el segundo relativo al deber de control de una fuente de peligro[539], el Código penal establece tres situaciones en las que puede aparecer la figura del garante: cuando exista una obligación legal o exista una obligación contractual (art. 11.a CP), y cuando el omitente haya creado una ocasión de riesgo para el bien jurídicamente protegido mediante una acción u omisión precedente (art. 11.b CP).

Respecto de las dos primeras posibilidades no cabe duda de que aparecerán con cierta frecuencia cuando entre en juego la figura de los administradores informáticos, o los técnicos informáticos (ya sea en la empresa privada o en la Administración Pública). Sin embargo, aún apuntado esto, no podemos afirmar que tal subsunción del administrador del sistema informático como el garante a efectos de la comisión por omisión deba ser absoluta, ni deba, por tanto, devenir siempre en una acción penal, incluso mediando un mandato de protección del propietario de los datos, programas informáticos o documentos electrónicos. La realidad de la informática demuestra que, en muchas ocasiones, el atacante tiene unos conocimientos que sobrepasan cuantitativamente los del administrador o

---

jurídico del autor, equivalga, según el sentido del texto de la Ley, a su causación. A tal efecto se equiparará la omisión a la acción: a) Cuando exista una específica obligación legal o contractual de actuar y b) Cuando el omitente haya creado una ocasión de riesgo para el bien jurídicamente protegido mediante una acción u omisión precedente".

[538] Requisitos reiterados por el Tribunal Supremo en su jurisprudencia: posición de garante, producción de resultado, posibilidad de haberlo evitado (SSTS 1093/2006 de 18 de octubre, 37/2006 de 25 de enero o 2392/2001 de 10 de diciembre entre muchas otras).

[539] MIR PUIG, S.: *Derecho…* ob. cit. pp. 321 y ss. y OCTAVIO DE TOLEDO Y UBIETO, E. y HUERTA TOCILDO, S.: *Derecho*… ob. cit. pp. 578 y ss.

administradores del sistema informático[540]. No podemos negar la posibilidad de que exista un supuesto garante, pero la realidad material de estos delitos va a hacer muy complicado imputar objetivamente a estos sujetos un eventual resultado de daños en comisión por omisión, salvo en aquellos casos en los que el administrador-garante haya actuado con verdadera falta de todo deber de cuidado en su labor o, de no existir tales administradores, la empresa que debería haber contado con ellos, se pueda convertir entonces en el autora directa del delito[541]. La falta de pericia, pues, de estos administradores informáticos, podrá dar lugar a la resolución contractual u otro tipo de sanciones (vía civil, laboral o administrativa), pero no constituirá en todos los casos, motivo suficiente para la imputación penal de los hechos en comisión por omisión.

[540] En general la gran mayoría de PYMES por motivos económicos obvios no cuenta con un equipo de ingenieros expertos en seguridad informática para administrar sus sistemas informáticos, sino técnicos de nivel medio, lo que las hace especialmente vulnerables a ataques.

[541] Véase un ISP (compañía que provee servicios de internet) que daña equipos de sus clientes por el tráfico de virus desde sus servidores. Aunque difícilmente podría imputarse la conducta en comisión por omisión a la compañía de forma general, es cierto que si ésta no hubiese tenido el cuidado mínimo para evitar tal resultado, como sería tener un equipo importante de técnicos dedicados a la seguridad informática (estas empresas son grandes compañías generalmente), podría atribuírsele la comisión del daño sobre los datos, programas informáticos o documentos informáticos. Es decir, podría aplicarse la doctrina de los "programas de cumplimiento normativo" para las personas jurídicas que ya ha comenzado a implantarse en nuestro ordenamiento en cuestiones relativas al blanqueo de capitales y otros delitos socioeconómicos (BACIGALUPO SAGGESE, S.: "Ética empresarial y Responsabilidad penal de las empresas" en *Encuentros multidisciplinares*, vol. 13, nº 39, 2011, pp. 3 y 4) en el ámbito de los delitos informáticos, y solo las empresas que incumplieran los mismos ocuparían la posición de garante, véase BACIGALUPO SAGGESE, S.: "Los criterios de imputación de la responsabilidad penal de los entes colectivos y de sus órganos de gobierno (arts. 31 bis y 129 CP)" en *La Ley*, nº 7541, 2011, pp. 2 y ss. A conclusiones similares llega ZUGALDÍA ESPINAR, J. M.: *La responsabilidad…* ob. cit. pp. 96 y ss. En el ámbito de nuestra investigación a situaciones de este estilo se refieren DE LA MATA BARRANCO, N. J, y HERNÁNDEZ DÍAZ, L.: "El delito…" ob. cit. p. 338, cuando señalan que si bien hay que descartar la omisión propia, no tanto la impropia, "así por ejemplo cuando los operadores, en posición de garantía, puedan tener conocimiento de que desde sus servidores se pueden estar cometiendo delitos de daños, pero, sobre todo, cuando sabiendo que se ha introducido una bomba lógica que se activara porque se ha rescindido, por ejemplo, un contrato de mantenimiento del sistema informático, no impiden la destrucción operada por el software malicioso". En el mismo sentido MATA y MARTÍN, R. M.: *Delincuencia…* ob. cit. p. 69 y CORCOY BIDASOLO, M.: "Protección penal del sabotaje informático. Especial Consideración de los delitos de daños*"* en *La Ley*, número 1, 1990. pp. 1011 y ss. De forma general, se refiere a la comisión por omisión de las personas jurídicas RODRÍGUEZ RAMOS, L.: "¿Cómo puede delinquir una persona jurídica en un sistema penal antropocéntrico? (La participación en el delito de otro por omisión imprudente: pautas para su prevención)" en *Diario La Ley*, nº 7561, 2011, pp. 6 y ss. de la edición electrónica.

En el art. 11.b CP se establece una tercera fuente de la posición de garante cuyo origen no se encuentra en la relación contractual o la imposición legal. Nos referimos al que se sitúa en posición de garante por el actuar precedente. En este caso es necesario que, por una acción u omisión, el garante haya creado una situación de riesgo para el bien jurídico protegido. Parece lógico que el que ha creado una situación de riesgo precedente, incurra en la posición de garante y por tanto en la obligación de evitar el resultado para no ser considerado autor por omisión[542]. Situación algo más compleja es aquel supuesto en el que un sujeto, utilizando el sistema informático de otro, visita una página web insegura o descarga contenidos dudosos que pueden producir daños en los datos, programas informáticos o documentos electrónicos del propietario del sistema informático. En este caso, el actuar precedente de este sujeto ha creado un peligro para el bien jurídico; y si bien no es él el que ha enviado el virus u otro *software* malicioso, cabría preguntarse si debería responder por los daños causados, o bien, el uso con consentimiento del propietario de los datos o el sistema informático excluye la tipicidad del resultado. La realidad, aun así, es que en el campo de la informática el desconocimiento sobre los riesgos sigue siendo elevadísimo, de tal forma que la creación imprudente de ese riesgo nos llevaría a plantear una situación límite a la hora de subsumir al sujeto en la posición de garante, pues sería complicado entender que ha podido surgir la infracción de la norma de cuidado. Más si cabe si consideramos que el consentimiento puede actuar como causa de atipicidad en la comisión activa del delito -y por tanto también en modalidad omisiva- por cuanto en el momento en que el uso del sistema informático ajeno se hiciera con el beneplácito del propietario, parecería difícil abarcar todos los elementos típicos del tipo[543].

Dicho esto, lo cierto es que el Código penal en su artículo 11 no establece que el riesgo producido para el bien jurídico se deba cometer exclusivamente de forma consciente, debido a lo cual la producción imprudente de esa situación de peligro

[542] MIR PUIG, S.: *Derecho…* ob. cit. p. 324 y ZUGALDÍA ESPINAR, J. M.: *Fundamentos*… ob. cit. pp. 480 y ss.

[543] FLORES PRADA, I.: *Criminalidad…* ob. cit. p. 175, señala que el consentimiento excluye la comisión por omisión, refiriéndose especialmente a los casos de reparaciones de técnicos que no son capaces de evitar que finalmente se produzcan daños informáticos, por ejemplo al no haber sido capaces de detener la ejecución de un virus informático o una bomba lógica.

podría quedar igualmente recogida, aunque tal situación deviene en una discusión doctrinal compleja[544]. Por ello, sería más adecuado subsumir tal acción dentro de una hipotética figura de daños informáticos imprudentes en su modalidad activa siempre que estos se reputasen graves. Remitiéndonos entonces a lo que sobre la posible existencia de un tipo penal de daños informáticos imprudentes sostengamos en las próximas páginas.

En relación con lo dispuesto en el artículo 11.b CP aparece también la figura del sujeto que con conocimientos informáticos, detecta en un sistema informático un virus o *software* malicioso que va a producir un daño futuro. Surge aquí la cuestión sobre si este sujeto está obligado a evitar la causación del resultado, es decir, si se convierte de forma sobrevenida en garante debido a su rol particular en esa determinada situación o, por el contrario, no podría hacérsele responsable del daño informático futuro. No parece existir duda de que en estos casos, si el sujeto actúa cumpliendo con el pertinente deber de cuidado, tratando en primer lugar de evitar el resultado, e informando al propietario de los datos, programas informáticos y documentos electrónicos del peligro existente, no podría imputársele el resultado en comisión por omisión. Por el contrario, si conociendo el peligro existente, no hace nada para evitar el resultado, podrían imputársele en comisión por omisión los daños informáticos producidos[545].

Por último, sin ubicarse sistemáticamente en el inciso a) ni en el b) del artículo 11 CP, no se puede descartar la asunción voluntaria de la situación de garante, que puede producir que un sujeto con conocimientos en informática y en base a una relación personal (o análoga) con el sujeto pasivo trate de evitar unos daños informáticos en su sistema informático. Esta situación no está resuelta de forma clara por la doctrina, y deberá ser siempre contrapuesta a lo ya analizado referente al riesgo permitido y el consentimiento, pues en estos casos (al igual que en los anteriores en los que el garante actúa cumpliendo los deberes exigidos por su rol) parecería contraproducente castigar penalmente a aquel que, voluntariamente,

[544] MIR PUIG, S.: *Derecho…* ob. cit. p. 327. Con matices, HUERTA TOCILDO, S.: *Principales*… ob. cit. pp. 45 y 46. Extensamente, de nuevo, en DOPICO GÓMEZ-ALLER, J.: *Omisión*… ob. cit.

[545] De nuevo DE LA MATA BARRANCO, N. J, y HERNÁNDEZ DÍAZ, L.: "El delito…" ob. cit. p. 338, y MATA y MARTÍN, R. M.: *Delincuencia…* ob. cit. p. 69.

tratando de evitar los efectos de un virus informático u otro *software* malicioso, finalmente no consigue evitar el daño. En este sentido, parte de la doctrina conviene en reconducir la situación a través de una ficción a la figura del contrato del artículo 11.a CP[546], de tal manera que como ya enunciábamos antes, la producción final del resultado podría acarrear consecuencias entre el sujeto pasivo y el supuesto garante, que si bien podrían tener naturaleza penal, probablemente serían mejor resueltas en el orden extrapenal (responsabilidad civil, responsabilidad laboral, etc.).

Con respecto a la figura del artículo 264.2 CP, parece, igualmente, que ese garante al que se le pudiera imputar la causación del resultado, que en este caso sería la interrupción u obstaculización de los sistema informáticos, podría ser el mismo sujeto, o similares, a los del párrafo primero. Lo que nos llevaría a los mismos problemas y soluciones que en el apartado anterior hemos planteado relativos a la interpretación respecto de una posible imputación en los supuestos previstos en el artículo 11 del Código penal. En todo caso, al margen de la casuística particular, y la conveniente valoración de los tribunales caso por caso podría, en principio, contestarse afirmativamente (quizá incluso con mayor frecuencia de lo que pueda parecer) sobre la posibilidad de la comisión por omisión en este tipo de delitos[547].

b.4. Grado de ejecución.

Uno de los problemas que derivan del delito de daños informáticos es el de conocer el momento de la perfección del delito. Es común que entre la actuación del sujeto activo y la producción del resultado pueda ocurrir un *iter* de tiempo en muchas ocasiones prolongado en el que la ejecución del delito queda en suspenso. Lo que nos lleva a preguntarnos cuándo efectivamente se produce la consumación del delito. A este respecto parece indicado someterse a la teoría general del delito como medio común de resolución de estas situaciones[548]. Es decir, la consumación del delito no se produce hasta que se verifica el resultado previsto, que en este caso es el daño sobre

[546] MIR PUIG, S.: *Derecho*... ob. cit. p. 323, "un sector de la doctrina cree preferible todavía […] acudir a la idea de contrato".

[547] GONZÁLEZ RUS, J. J.: "El cracking…" ob. cit. p. 243.

[548] Respecto de los artículos 16.1 y 16.2 CP, véase DE LA MATA BARRANCO, N. J.: "El delito…" ob. cit. pp. 172 y 173.

datos, programas informáticos o documentos electrónicos, o la interrupción u obstaculización de los sistemas informáticos.

El delito permite tipos de imperfecta realización en cuanto a la tentativa se refiere, así como la anudada posibilidad del desistimiento de la tentativa[549]. Nada impide en estos tipos en concreto, además, que la tentativa pueda igualmente producirse de manera acabada o inacabada, aunque la situación más frecuente en la práctica será aquella en la que la tentativa sea acabada, pues el atacante haya realizado todos los elementos del tipo, y sólo por causas ajenas a él, como un sistema de seguridad informático adecuado de las víctimas, se evie la terminación normal del ataque al bien jurídico[550].

Cuestión a discutir sobre este extremo es la figura, común hoy en día, de las copias de seguridad o *backups*[551]. Sobre este particular, la existencia de estas copias de seguridad suscita dos posiciones enfrentadas. La primera, afirma que la existencia de dichas copias de seguridad elimina absolutamente la posibilidad de la consumación del resultado[552], dejando entrever que de no haberse producido un daño definitivo (no hay permanencia del daño[553]) lo correcto es incardinar siempre tales

[549] CORCOY BIDASOLO, M.: *Protección…* ob. cit. pp. 1014 a 1016.

[550] MIR PUIG, S.: *Derecho…* ob. cit. pp. 355.

[551] Se entiende por copia de seguridad o *backup* la realización de una copia exacta del contenido de un sistema informático en un soporte normalmente externo al propio sistema informático; de tal manera que dicha copia exacta sirva de respaldo en caso de que se produzca un daño (provocado o no provocado) en el sistema informático original. Habitualmente las copias de seguridad suelen referirse exclusivamente a los documentos electrónicos, y no tanto a los programas informáticos que gestionan los sistemas informáticos. Aunque como hemos mencionado existen copias de seguridad que crean una copia de respaldo que reproduce exactamente igual el sistema informático respaldado.

[552] Es la tesis que mantiene GONZÁLEZ RUS, J. J.: "Protección…" ob. cit. (sin numerar), "la destrucción, la alteración, la inutilización o el daño han de comportar la alteración definitiva de la integridad de los datos, haciendo imposible su utilización o restauración tal y como estaban antes de la realización de la conducta. Como consecuencia, deberá apreciarse la tentativa tanto cuando el virus, la bomba lógica o el procedimiento utilizado para causar los daños no llega a activarse, como cuando existan copias de respaldo o copias de seguridad de los ficheros o de los datos dañados, lo que hace que éstos puedan ser reincorporados al sistema o a la red sin especiales dificultades o existen otras copias del programa que permiten su reinstalación".

[553] MORALES GARCÍA O.: "Comentario a los delitos informáticos de los arts. 197, 248 y 264 CP" en VV.AA.: *Delincuencia informática. Tiempos de cautela y amparo,* Ed. Thomson Reuters Aranzadi, 1ª edición, Navarra, 2012, p. 158, también observa que "no existe diferencia entre original y copia de manera que los datos o programas pueden ser copiados infinitamente lo que liga con la extraordinaria

conductas en las diferentes figuras de la tentativa[554]. Contra esta línea de pensamiento se plantean otros autores el hecho de que aun existiendo una copia de seguridad de los datos, podría ésta encontrarse físicamente en otro lugar (de hecho, eso sería lo aconsejable) de tal forma que reconstruir todos los sistemas informáticos después de un ataque supondría un considerable perjuicio económico. Conforme a esta postura doctrinal el problema se incardina, como ya se ha manifestado en esta investigación, en que el perjuicio económico que causa la recuperación de los sistemas, y el lucro cesante, deben ser daños sujetos a la responsabilidad civil y no penal[555], pues la protección penal encuentra su fundamento en el daño a unos datos, programas informáticos o documentos electrónicos que, al tener una copia de respaldo, no han perdido su valor económico pues se encuentran intactos (aunque alojados en otro lugar diferente al natural para su utilización). Aceptar que estos daños sí se subsumen en el tipo objetivo supondría, una vez más, enfocar de una nueva manera el bien jurídico protegido por estos delitos[556] y su interpretación, postura defendida en este trabajo y a la que dedicaremos la tercera parte de la investigación.

Por último, también se ha suscitado aisladamente en la doctrina la posibilidad de diferenciar o no entre originales y copias para entender consumado el tipo[557], cuestión que al menos desde un punto de vista técnico (lógico) no puede ser compartida por cuanto copia y original son exactamente iguales, hasta el punto de que llegado un momento determinado, puede darse el caso de no poder concretarse cuál es el objeto original y cual la copia.

---

capacidad de recuperación de los datos o programas informáticos", y determina que ello "casa dificilmente con la exigencia de un atentado a la sustancia de la cosa, propia de los delitos de daños".

[554] BUENO ARÚS, F.: "El delito informático*"* en *Actualidad Informática Aranzadi*, nº 11, 1994, p. 5 y MATA y MARTÍN, R. M.: *Delincuencia*… ob. cit. pp. 74 y ss.

[555] GONZÁLEZ RUS, J. J.: "Protección…" ob. cit. (sin numerar), "a ello debe añadirse que la determinación de la cuantía conforme a la que tipificar el hecho como delito o falta sólo puede hacerse en atención a la pérdida de valor real de la cosa derivada de su menoscabo sustancial, porque la apelación al valor de uso supone confundir el daño a la cosa con el perjuicio, cuya presencia no resulta determinante para la configuración del delito […]. Como consecuencia, la cosa debe ser valorada objetivamente, quedando excluidos a efectos de cuantía los perjuicios y los daños morales".

[556] RODRÍGUEZ MOURULLO, G., LASCURAIN SÁNCHEZ, J. A. y ALONSO GALLO, J.: *Derecho…* ob. cit. p. 285 y ss.

[557] GÓMEZ MARTÍN, V.: "Sabotaje…" ob. cit. p. 3.

b.5. Autoría y participación.

En cuanto a los modos de autoría, participación y actos preparatorios el artículo se sujeta a las reglas generales del Código penal.

Sobre el caso de los actos preparatorios, de alguna manera, la regulación internacional a través del Convenio sobre la Ciberdelincuencia de Budapest de 2001 exigía que se tipificasen en materia penal algunas acciones de este tipo. Acciones que la Decisión Marco 2005/222/JAI ha omitido al adaptar dicho Convenio al espacio europeo, y que nuestro Código penal tampoco regula[558]. Así, el Convenio internacional establece que deben ser castigados aquellos actos relacionados con la producción, comercialización o posesión de dispositivos que permitan o faciliten la realización de las acciones anteriormente recogidas por el Convenio (en nuestro caso las que regula como interferencia en el sistema -artículo 5- e interferencia en los datos, artículo 4). En todo caso exime a los legisladores nacionales de la obligación de utilizar el Derecho penal en los casos de producción y de posesión, pero sí exige taxativamente que sean castigados los actos relativos a la distribución de dichos dispositivos[559].

Como ya avanzamos, es curioso que ni la Decisión Marco ni, especialmente, el legislador español, hayan traspasado estas exigencias a sus regulaciones, más aún cuando los Convenios internacionales ratificados deben ser cumplidos por los Estados. De lo que no cabe duda, es que nuestro legislador tarde o temprano tendrá que tipificar tales conductas si pretende cumplir las exigencias que de la ratificación de dicho Convenio se derivan. En ello ahondará la próxima aprobación en sede europea de la Directiva que sustituirá a la Decisión Marco actual, a la que ya nos referimos en el capítulo segundo de esta investigación, que sí recogerá la exigencia de tipificación de las prácticas descritas.

Lo cierto es que los actos preparatorios como tales que recoge nuestro Código, es decir la conspiración, la proposición y la provocación para delinquir tipificados en los artículos 17 y 18 CP, sólo serán punibles en los casos que así lo

[558] DE LA MATA BARRANCO, N. J.: "El delito…" ob. cit. p. 172.

[559] Artículo 6 del Convenio de Ciberdelincuencia de Budapest de 2001.

establezca expresamente el propio Código. No existiendo por tanto remisión expresa, tales conductas no son sancionadas en nuestro ordenamiento penal respecto de los daños informáticos[560].

En todo caso, según queda establecida la configuración del Derecho penal español, éste castiga penalmente no sólo el autor material del hecho, sino también otros modos de autoría y participación. El artículo 27 del Código penal establece que son penalmente responsables los autores y los cómplices, y a continuación en el artículo 28 CP se establece la posibilidad de la autoría mediata y la coautoría, así como de otras formas de intervención como la inducción y la cooperación necesaria[561]. El artículo 61 del Código penal establece la misma pena a efectos sancionadores para los autores, inductores y cooperadores necesarios, y la inferior en grado para los cómplices. El tipo del artículo 264 CP no tiene especiales complicaciones en estos puntos, deberán ser los tribunales los que determinen en cada caso cual es la posición que ocupan los sujetos que han intervenido en el delito, siendo quizá está la forma de castigar penalmente a creadores o divulgadores de virus informáticos o *software* malicioso, no tanto por esa acción en sí, sino como por su labor necesaria al crear dichos programas para la ejecución posterior de los daños informáticos, como una suerte de cooperadores necesarios.

Por último, la autoría mediata en este tipo de delitos es perfectamente apreciable, y, en muchas ocasiones, puede ser la forma habitual de realización de los hechos. Piénsese en una situación en la que un sujeto envía un virus informático a un ordenador, en el que no se produce ningún daño hasta que el usuario de ese sistema informático realiza una acción determinada (método de acción de las bombas lógicas). Esta situación no lleva al usuario que ha realizado la acción a la posición de sujeto activo, muy al contrario, dicho usuario, aun siendo el autor material del hecho, ha actuado sin libertad ni conocimiento de la situación, circunstancia que sabía el

[560] Sobre ello se manifiesta GONZÁLEZ RUS, J. J.: "El cracking…" ob. cit. pp. 242 y 243, negando que la creación o difusión de virus pueda tener cabida dentro de las acciones típicas reguladas en nuestro Código penal.

[561] Son partícipes que el Código penal, conforme a lo establecido en el artículo 28, eleva a la categoría de autores.

autor mediato para favorecerse y producir el daño[562]. Más interesante puede resultar conocer cuándo se produce la acción típica del autor mediato, si en el momento en que él completa la acción que se le presupone como autor mediato, o si ésta no se produce hasta que el autor inmediato efectivamente realiza la acción típica[563]. La especial naturaleza de estos delitos recomienda no dar por absoluta una hipótesis, por lo que parece la solución más prudente esperar a conocer exactamente los hechos concretos y la participación exacta de cada parte en este tipo de casos.

C) ANÁLISIS DE LOS SUJETOS

c.1. Sujeto activo.

El delito de daños informáticos se configura como un delito común, por lo que el sujeto activo del mismo puede ser cualquier persona física[564] o jurídica, siempre que no sean los titulares de los datos, programas informáticos, documentos electrónicos o sistemas informáticos ya que rige la necesidad de ajenidad a los mismos[565].

Con respecto a esto último, la doctrina ha precisado que sería difícil incardinar en el delito de realización arbitraria del propio derecho del artículo 455 del

[562] Imaginemos el caso de quien distribuye un troyano (virus que se hace pasar por un programa común), recomendando a los usuarios que lo envíen a sus contactos. MIR PUIG, S.: *Derecho…* ob. cit. p. 382. Más extensamente OCTAVIO DE TOLEDO Y UBIETO, E. y HUERTA TOCILDO, S.: *Derecho…* ob. cit. pp. 483 y ss.

[563] A este respecto cabe destacar el análisis en SÁNCHEZ-VERA GÓMEZ-TRELLES, J.: "Sobre la figura de la autoría mediata y su tan sólo fenomenológica trascendencia" en *Anuario de derecho penal y ciencias penales*, nº 51, 1998, pp. 319 y ss., que concluye que tales distinciones no deben suponer, en la práctica, un problema de determinación de la autoría final del delito.

[564] Aunque no siempre es necesario que el sujeto activo tenga grandes conocimientos en informática o telecomunicaciones, la mayor preocupación de los Estados radica en las prácticas llevadas a cabo desde asociaciones o grupos de piratas informáticos (*hackers o crackers)*, cuyos objetivo, además, no siempre está directamente vinculado al beneficio patrimonial suyo o de un tercero, sino al activismo político. Sobre el perfil de estos sujetos, véase GALLARDO RUEDA, A.: "Delincuencia informática: la nueva criminalidad de fin de siglo" en *Cuadernos de política criminal*, nº 65, 1998, p. 372. En el mismo sentido ROMEO CASABONA, C. M.: "Delitos…" ob. cit. pp. 438 y 439, considera que "junto a estos daños [daños con finalidad de causar un perjuicio económico] no son desdeñables tampoco los que se pueden irrogar con finalidad política contra la seguridad y defensa de los Estados".

[565] Por todos MIRÓ LLINARES, F.: *Delitos…* ob. cit. p. 160.

Código penal[566] al sujeto que daña sus propios datos, programas informáticos o documentos electrónicos, o interrumpe u obstaculiza un sistema informático propio para evitar así otras consecuencias. Tal artículo exige que se actúe con violencia, intimidación o fuerza en las cosas. Ante la ausencia de soluciones jurisprudenciales y doctrinales al respecto, creemos que resultaría complicado insertar las acciones del tipo en la figura de "fuerza en las cosas", especialmente por el carácter inmaterial de los objetos. Subsumir las acciones dentro de un tipo de fuerza sobre las cosas inmateriales supone una interpretación demasiado extensiva del término, lo que nos lleva a la conclusión de que lo más adecuado, si se pretende perseguir penalmente dichas conductas, sería reformular el citado artículo 455 CP para dar cabida a los supuestos de los daños informáticos causados por el titular de los propios bienes[567].

Ya en otro orden de cosas, podemos afirmar que el sujeto activo no tiene por qué tener necesariamente conocimiento de la víctima del delito, lo que será habitual, sino saber que se actúa sobre objetos ajenos. El sujeto que actúa bajo el error de pensar que los datos, programas informáticos, documentos electrónicos o sistemas informáticos son de su titularidad caería bajo la figura del error de tipo[568].

Por lo que respecta a la posibilidad de que las personas jurídicas sean sujetos activos del delito, se regula en el apartado cuarto del propio artículo 264 CP, en el que se remite al artículo 31 bis (y otros) del Código penal para completar la regulación. En efecto, la realización de estas prácticas por personas jurídicas puede convertirse realmente en el campo de batalla donde se cometan estos delitos en los próximos años. Situaciones que van más allá de la defensa de la competencia y que

[566] Artículo 455 CP: 1. El que, para realizar un derecho propio, actuando fuera de las vías legales, empleare violencia, intimidación o fuerza en las cosas, será castigado con la pena de multa de seis a doce meses. 2. Se impondrá la pena superior en grado si para la intimidación o violencia se hiciera uso de armas u objetos peligrosos.

[567] DE LA MATA BARRANCO, N. J.: "El delito…" ob. cit. p. 165.

[568] El sujeto actúa conociendo la prohibición, pero desconoce uno de los elementos del tipo, que es la ajenidad, pues cree que es titular de dicho objeto. Tal situación parece no tener problemas en incardinarse dentro del error sobre un elemento esencial, que es el de la ajenidad. Dicho error podrá ser vencible o invencible, cuestión a valorar en cada caso. MIR PUIG, S.: *Derecho…* ob. cit. pp. 268 y ss.

deben ser analizadas en sede penal[569]. Dicha regulación parte de las exigencias del Convenio sobre la Ciberdelincuencia de Budapest de 2001[570], aunque de la lectura de su articulado no parece desprenderse claramente que la exigencia de que se haga responsables a las personas jurídicas llegue a obligar a los Estados a que dicha responsabilidad se constituya en sede penal. Así, establece en el apartado primero que "cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para que pueda exigirse responsabilidad a las personas jurídicas por los delitos previstos de conformidad con el presente Convenio", pero ello no indica que esa responsabilidad no pueda ser de otro tipo a la responsabilidad penal. Totalmente aclarado queda este extremo cuando, el apartado tercero de dicho artículo, establece ya explícitamente que "con sujeción a los principios jurídicos de cada Parte, la responsabilidad de una persona jurídica podrá ser penal, civil o administrativa". De tal manera que la configuración del propio Convenio establece únicamente como imperativo la responsabilidad penal de las personas físicas, y la responsabilidad en general (no necesariamente penal) de las personas jurídicas por los actos de las personas físicas que actúan en ella. Exactamente en los mismos términos queda redactado el articulado referente a las responsabilidades de las personas jurídicas en el ámbito de la Decisión Marco 2005/222/JAI de 24 de febrero[571], en el que tampoco se exige que la responsabilidad que deban afrontar las personas jurídicas sea estrictamente penal, aunque es cierto que a diferencia de la redacción del Convenio, tampoco clarifica las opciones entre las que puede elegir los legisladores nacionales. De lo que no cabe duda, es que conforme a la regulación por la que ha optado el legislador nacional, trata a las personas jurídicas como posibles sujetos activos de los tipos del artículo 264.1 y 264.2 CP, cuestión que entendemos acertada tal y como se ha desarrollado la responsabilidad penal de las personas jurídicas en nuestro Código

[569] Véase el ejemplo de una empresa que interrumpe los sistemas informáticos de otra empresa de la competencia, inutilizando su página web a través de la cual realiza el grueso de su negocio. Desviando sus posibles clientes a otras empresas y causando un perjuicio patrimonial considerable. Parecería escaso un reproche de índole mercantil por practicar la competencia desleal. O en el extremo más grave, la aparición de auténticas empresas criminales nacidas con el propósito de atentar contra objetivos informáticos de relevancia para los Estados.

[570] Artículo 12 del Convenio de Ciberdelincuencia de Budapest de 2001.

[571] Artículo 8 de la Decisión Marco 2005/222/JAI de 24 de febrero.

penal con la reforma de 2010[572], ateniéndonos a las circunstancias de que los tipos analizados aparecerán en no pocos casos vinculados a empresas mercantiles que traten por esta vía, principalmente, de alterar la competencia en los mercados.

c.2. Sujeto pasivo.

En lo que al sujeto pasivo del delito se refiere, deberá entenderse como tal el propietario de los datos, programas informáticos, documentos electrónicos -en los casos de apartado primero- o sistemas informáticos -en el apartado segundo-[573]. Pero sobre esta cuestión cabe realizar algunas puntualizaciones.

Partiendo de la idea de que estamos ante delitos contra el patrimonio, no cabe otra solución que atribuir al propietario del objeto la figura de sujeto pasivo, aunque, como es fácil de entender, no siempre será él el inmediatamente perjudicado o el usuario final de los datos, programas informáticos, documentos electrónicos o sistemas informáticos que se vean afectados. Esa situación se puede observar claramente en el caso de que se ataquen los sistemas de una empresa, cuya utilización corresponde a los empleados de la misma, pero que no se sitúan en la posición de sujetos pasivos, que será siempre la empresa propietaria de los mismos[574]. Pero la realidad de hoy en día nos obliga a preguntarnos si es adecuada esta identificación del sujeto pasivo con el propietario, véase el ejemplo de los programas informáticos online[575], más si cabe cuando son programas para cuya utilización el usuario ha tenido que pagar previamente (se paga por su acceso y uso, no por la propiedad del mismo). En estos casos el ataque a la integridad del programa informático normalmente no se realizará sobre el equipo del usuario, sino sobre los servidores de la compañía que sirve el programa a los usuarios. Dicho ataque, que deja sin servicio a los usuarios aunque no tengan instalado el programa en su equipo, les puede producir sin duda un perjuicio económico, más aún si han pagado por dicha

[572] Ley Orgánica 5/2010, de 22 de junio, por la que se modifica la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal.

[573] Por todos MIRÓ LLINARES, F.: *Delitos…* ob. cit. p. 160

[574] DE LA MATA BARRANCO, N. J.: "El delito…" ob. cit. p. 169.

[575] Nos referimos a programas que ejecutan ciertas funciones pero que no se encuentran integrados en el sistema informático desde el que se utilizan. Son los reproductores de video alojados en las propias webs como Youtube, los procesadores de textos online como Google Docs, o incluso los juegos online a los que se accede a través de Facebook, etc.

utilización o si la usan para fines empresariales; sin embargo, no son ellos en sentido estricto los propietarios de los mismos, por lo que sujetándonos a la interpretación de la figura del sujeto pasivo como propietario del objeto no podrían encajar en dicha figura. No hay duda de que esta situación expuesta no es la misma que la del empleado que usa el ordenador de su empresa y no puede seguir trabajando por culpa de un ataque al que nos referíamos con anterioridad. Lo que nos lleva a preguntarnos sobre la posición de estos delitos como tipos de daños, cuando pueden darse situaciones tan particulares como la ahora descrita, volviendo a suscitarse interrogantes respecto al bien jurídico protegido[576].

D) OBJETO MATERIAL

El mandato de taxatividad, y la evitación de conceptos jurídicos indeterminados adquieren especial relevancia a la hora de tratar el objeto material de los delitos de daños informáticos. Es importante recordar que el principio de legalidad penal exige, entre otras cosas, evitar la utilización de términos excesivamente amplios, ambiguos o indeterminados en la redacción de tipos penales. La inaprehensibilidad de los objetos del delito del artículo 264.1 CP es un factor que complica la labor del legislador a la hora de respetar está máxima aunque es cierto que el legislador tampoco puede utilizar la ley para definir cada término que en ella aparece[577], por ello debe ser labor de la doctrina -como de la jurisprudencia- puntualizar algunas cuestiones en cuanto a lo que se debe entender por datos, programas informáticos y documentos electrónicos -del artículo 264.1CP- y, con menos dificultad, por sistema informático -del artículo 264.2 CP-.

---

[576] A este respecto DE LA MATA BARRANCO, N. J.: "El delito…" ob. cit. p. 169, expresa que el debate debería centrarse en si el bien jurídico protegido es por tanto el patrimonio, o excede de este. En ese mismo sentido, y no sin falta de razón MARCHENA GÓMEZ, M.: *Internet…* ob. cit. pp. 363 y ss., se plantea la cuestión de si estamos ante un delito de daños, o una forma de desórdenes públicos.

[577] HUERTA TOCILDO, S.: "Principio…" ob. cit. p. 42, afirma que "tampoco está obligado el legislador penal a acuñar definiciones específicas para todos y cada uno de los términos que integran la descripción típica" sin embargo añade que sí parece necesario "cuando utilice términos que, por su falta de arraigo en la cultura jurídica, carecen de toda virtualidad significante y cuyo contenido semántico no puede ser concretado con ayuda de criterios lógicos, técnicos o de experiencia". La pregunta giraría en torno a saber si los objetos materiales de estos delitos se encuentran entre alguna de estas posibilidades, o si la interpretación ´jurídica´ debe diferir de la técnica, consecuencia de lo cual resultaría interesante introducir definiciones en el tipo penal, como, por otro lado, ya realiza para algunos conceptos la regulación internacional en la materia.

En primer lugar vamos a delimitar los conceptos de datos, programas informáticos y documentos electrónicos, objeto material al que alude el apartado primero del artículo 264 CP. El "dato" al que se hace constante referencia en la legislación internacional y también en nuestro propio Código penal no responde a concepto tradicional de dato[578]. Debemos suponer que cuando de regulación de cuestiones informáticas se trata, se utilizan los términos con su significado informático. Cuando el tipo penal sanciona el borrado de datos (de carácter informático recordemos), no se refiere a la idea normal de borrar, por ejemplo, un número de teléfono de un documento, porque ese número de teléfono no es un dato en sentido informático (aunque esa acción podría ser típica por vía de la alteración de un documento electrónico). Los datos serían los -millones de- *bits* que conforman la representación visual en un sistema informático de ese número de teléfono. Por ello, quizá lo más adecuado para fijar un punto de partida para interpretar el artículo es entender dato, como *bit*[579], es decir como la unidad mínima de información utilizada en informática[580].

Establecido lo anterior, nos encontramos con que tanto el Convenio sobre la Ciberdelincuencia de Budapest de 2001 como la Decisión Marco 2005/222/JAI de 24 de febrero deciden dar una definición de dato informático que más que aclarar dudas las aumenta[581]. En efecto dicha definición (nos centraremos en la de la Decisión

---

[578] Hace una descripción acertada desde una perspectiva técnica GONZÁLEZ RUS, J. J.: "Protección…" ob. cit. (sin numerar), "«Datos» son las unidades básicas de información, cualquier que sea su contenido (un número, una palabra, un sonido, una imagen) y que al ser procesadas dan lugar a la "información", que resulta de la conexión entre dos o más datos". En la misma línea, hace más de dos décadas, SNEYERS PODOLSKY, A.: *El fraude y otros delitos informáticos*, Ed. Tecnologías de Gerencia y Producción, 1ª edición, Madrid, 1990, p. 111.

[579] En realidad *bit* es el diminutivo de *binay digit*, definido como la unidad de medida más pequeña que un sistema informático puede procesar. S.M.H COLLIN: *Dictionary…* ob. cit. p. 37.

[580] En esta línea se manifiesta muy acertadamente DE LA MATA BARRANCO, N. J.: "El delito…" ob. cit. p 170, "los datos son, en síntesis, unidades básicas de información que después de ser procesadas dan lugar a una información".

[581] El Convenio sobre la Ciberdelincuencia de Budapest de 2001 establece que por dato informático "se entenderá cualquier representación de hechos, información o conceptos de una forma que permita el tratamiento informático, incluido un programa diseñado para que un sistema informático ejecute una función". Con una definición casi exacta la Decisión Marco 2005/222/JAI establece que dato informático será "toda representación de hechos, informaciones o conceptos de una forma que permite su tratamiento por un sistema de información, incluidos los programas que sirven para hacer que dicho sistema de información realice una función".

Marco pues es la que más cercana queda a nuestra regulación penal) no equipara la idea de dato a la de unidad mínima de información, sino que decide que sea "toda representación de hechos, informaciones o conceptos de una forma que permite su tratamiento por un sistema de información". Y sobre esta definición deben trabajar los jueces y tribunales de los Estados, así como la doctrina, cuando se analicen las figuras de delitos informáticos en los procesos judiciales o en el ordenamiento jurídico penal. Es decir, que un dato según la interpretación legal, no es la unidad mínima de información, sino algo un poco más amplio, sin determinar cuánto más amplio, llegando incluso a confundirlo con el concepto de programa informático, cuando un programa informático en ningún caso puede equipararse a un dato, sino más bien y en todo caso, a un grupo de varios -millones- de datos. Se genera, a partir de esta definición una inseguridad jurídica que la doctrina debe tratar de solventar, de forma que facilite la labor de los operadores del derecho a la hora de enfrentarse ante estos delitos.

Por eso creemos que, a pesar de esta definición legal que se establece, igualmente se debe reconducir dicho concepto a la idea de dato que avanzamos anteriormente, es decir, la de *bit*. Se puede criticar, sin lugar a dudas, que utilizar un concepto tan concreto en el sentido técnico (pero tan amplio en el sentido de que cualquier orden informática por pequeña que sea ya podría ser merecedora de protección penal) como es el que se sujeta a la definición de *bit* (unidad mínima de información con la que trabaja un sistema informático) puede dar lugar a sobredimensionar la parcela penal[582]. No obstante, para evitar dicha situación existen otras barreras que el legislador puede utilizar y de hecho ha utilizado al prever como reprochables sólo aquellas conductas que tengan un resultado grave.

Siguiendo esta definición por tanto, el dato informático o *bit* según la teoría de la informática, es poseedor de dos tipos de información: positiva y negativa. De tal forma que sobre un único dato sólo se puede realizar una acción, que es la de alterar su posición de positiva a negativa o viceversa, o bien hacerlo inaccesible a

[582] MIR PUIG, S.: *Derecho…* ob. cit. pp. 116 y ss. En muchas ocasiones la alteración de un solo bit no produce efecto alguno sobre la representación visual en el sistema (modificar un sólo bit en una fotografía no produciría en la mayoría de los casos el más mínimo resultado), y aun así podría producir la acción típica si no fuese porque no es capaz de cumplir el resto de requisitos típicos.

través de un medio externo. Este razonamiento, que es puramente teórico, encuentra una crítica en el plano de la realidad, y más en el orden penal, y es que nunca se trata de dañar un solo dato, pues lo que se pretende normalmente con el daño, y ya se ha puesto de manifiesto a lo largo de esta investigación, es modificar la funcionalidad de un programa o la integridad de un documento que supone una cantidad infinitamente grande de datos agrupados con una determinada estructura[583]. Quizá por esta razón el legislador internacional ha pretendido en su definición de dato informático tratar de señalar el propio dato como algo más grande que un solo *bit*, con el problema que ya hemos apuntado de incurrir en el error de dar una definición que no aclara el concepto de manera práctica. Por ello, más importante que el dato informático es en realidad el significado que se le dé a documento electrónico o programa informático. Por lo menos por dos razones: una práctica, y es que siendo acertados en sus correctas definiciones podemos excluir la problemática que surge de la protección penal del concepto de "dato", y otra; de carácter jurídico, para evitar el complicado mundo que se abre a la hora de valorar el perjuicio patrimonial que supone modificar un solo dato -*bit*-, que sería cuanto menos insignificante y por lo tanto no merecedor de protección penal.

Programa informático y documento electrónico son los otros dos términos a los que nos referimos constantemente y son los realmente importantes. Deben ser entendidos aquí como una sucesión ordenada de datos informáticos -*bits*- que se traducen al final de su procesamiento en objetos lógicos inteligibles por el usuario del sistema informático o que de alguna manera repercuten en el sistema informático de forma apreciable en el presente o el futuro. Un programa informático se caracteriza por su funcionalidad para muy variados propósitos[584] y un documento

[583] En informática 8 bits de información conforman 1 byte, 1 byte de información 1024 Kb y 1024 Kb información es 1 Mb, que ya comienza a ser una unidad que todos conocemos y manejamos a nivel usuario. Debemos ser conscientes de que un documento electrónico, y especialmente un programa informático, pueden ocupar cientos de Mb, es decir millones de *bits.*

[584] Parece adecuado acudir al Texto Refundido de la Ley de Propiedad Intelectual para confirmar la corrección de la definición referida "Art. 96.1. A los efectos de la presente Ley se entenderá por programa de ordenador toda secuencia de instrucciones o indicaciones destinadas a ser utilizadas, directa o indirectamente, en un sistema informático para realizar una función o una tarea o para obtener un resultado determinado, cualquiera que fuere su forma de expresión y fijación." FARALDO CABANA, P.: *Las nuevas técnologías en los delitos contra el patrimonio y el orden socioeconómico*, Ed. Tiran Lo Blanch, 1ª edición, Valencia, 2009, p. 140.

electrónico se caracteriza por contener algún tipo de información visual, acústica, etc.

Con respecto a la acepción "programa informático" parece correcto asumir que por tal expresión el legislador se refiere al término clásico de *software*. Con el deslinde que ocurre en el mundo de la informática durante los años sesenta entre *hardware*, que son los componentes físicos del sistema informático, y *software*, o componentes lógicos que consiguen que los primeros puedan ser utilizados[585], se produce la necesidad de proteger también por separado los ataques a ambos objetos. En nuestra tradición penal, al igual que en el caso de los documentos electrónicos, se ha comentado poco su posición como objeto material de los delitos. Es cierto que, a diferencia de la figura que veremos a continuación, se ha tratado un poco más en profundidad, pero siempre en relación a los delitos de propiedad intelectual, y en general, en el ámbito jurídico, ya sea penal o civil, siempre se ha estudiado el *software* y su protección desde la perspectiva de los derechos de autor[586].

La cuestión que ahora nos ocupa, referida a determinar el objeto material del tipo del artículo 264.1 del Código penal debe centrarse en el ámbito del delito de daños y en verificar lo que el legislador realmente pretende proteger. Desde luego con la inclusión de este tipo no trata de tutelar el hecho de que sobre un programa del que no se tienen los derechos de autor necesarios se operen modificaciones en el sentido intelectual (realización de obra derivada, reproducción pública, plagio, etc.), cuestiones que se derivarían a la propiedad intelectual -bien por vía penal, bien por la civil-. No nos encontramos, por tanto, ante una ley penal en blanco que remite para la interpretación del concepto a otra normativa, por ejemplo la Ley de propiedad

[585] De forma muy resumida DAVARA RODRÍGUEZ, M.A.: *Manual…* ob. cit. p. 115. Para un conocimiento exhaustivo se recomienda O'REGAN, G.: *A brief…* ob. cit.

[586] La regulación del *software* se realiza en nuestro ordenamiento a través del Texto Refundido de la Ley de Propiedad Intelectual, al que dedica su Título VII (artículos 95 al 104).

intelectual[587], porque lo que se pretende proteger es, en realidad, la funcionalidad de ese programa, su utilidad, el fin por el que ha sido creado[588].

Expresado de esta manera, lo que realmente tienen un valor cuantificable económicamente, y es protegido por este artículo, no son el conjunto de los datos que conforman un programa de ordenador, sino las funciones que ese programa lleva a cabo. Es decir, lo que el legislador trata de proteger con el artículo 264.1 CP es el valor de las funciones que lleva a cabo el programa informático[589] y no la integridad del programa informático en sí. De tal forma que como ya se analizó en el estudio de las acciones típicas, una alteración de un programa que aumenta sus funciones y deja intactas las que ya posee podría no ser típica si entendemos que el bien protegido es el patrimonio (esto es, su valor económico) y que, por tanto, no se ha atacado a su funcionalidad original; sin necesidad de acudir a verificar otros elementos como la aparición de un resultado, etc[590]. Debemos concluir en este caso que el objeto material por tanto, no es el programa o *software* como tal, sino la funcionalidad del mismo.

De los tres posibles objetos materiales del primer apartado del artículo 264 CP es preciso realizar un breve apunte sobre el concepto de documento electrónico. Como ya avanzamos al respecto, el documento electrónico en general es aquel que contiene una información de algún tipo en formato electrónico. La doctrina, en su

[587] Real Decreto Legislativo 1/1996, de 12 de abril, por el que se aprueba el texto refundido de la Ley de Propiedad Intelectual, regularizando, aclarando y armonizando las disposiciones legales vigentes sobre la materia.

[588] Así lo entienden RAGUÉS I VALLES, R. y ROBLES PLANAS, R.: "La reforma…" ob. cit. p. 374, al señalar que el daño se fundamente en el "menoscabo de la función o utilidad a la que está destinada la cosa", o QUERALT JIMÉNEZ, J. J.: *Derecho…* ob. cit. p. 641.

[589] No se trata de sancionar la alteración de un programa, sino que un programa que realiza una función, por ejemplo hacer funcionar un cajero automático, sea alterado (o dañado en sentido amplio) de tal forma que ya no realice esa función, o la realice mal. En el ejemplo del cajero sería alterarlo de tal manera que cuando pidamos sacar billetes de 20 nos los entregue de 50. Por ello, lo correcto no es sancionar el daño a un programa informático, sino el daño sobre la función que desarrolla ese programa informático. FLORES PRADA, I.: *Criminalidad…* ob. cit. pp. 172, 179 y ss.

[590] En el ejemplo del cajero, si uno altera el programa que lo gestiona para conseguir poder elegir el tipo de billetes que le van a ser entregados (20 euros en billetes de 5, en lugar de un billete de 20 euros o dos de 10 euros), difícilmente podríamos decir que se haya producido una acción típica del 264.1 CP, ya no porque no se haya producido un resultado grave, sino porque la propia acción no ha alterado la funcionalidad del programa del cajero que es el verdadero objeto protegido.

mayoría civilista[591] ha venido a diferenciar entre documentos electrónicos y documentos informáticos. Aunque es cierto que el uso común a la hora de referirse a a los mismos es alternativo, se suelen diferenciar los documentos informáticos por ser una categoría más amplia de los electrónicos[592]. Son, en lo que interesa a la materia penal, por un lado los documentos electrónicos generados por medios informáticos, y por otro lado, aunque con matices, los físicos que han sido incorporados a un sistema informático por algún medio técnico (por ejemplo escanear una foto). Quedan fuera de la protección penal aquellos documentos que siendo en origen electrónicos se encuentran ahora en soporte físico directamente inteligible[593], si bien esta situación ha generado alguna discusión (con bastante razón), aunque su debate escape ahora de nuestro objeto de estudio[594]. Como se ha avanzado, la doctrina penalista no ha tenido excesiva participación en la creación del concepto de documento electrónico, de tal manera que todos los extremos que han sido tratados por los autores tienen por objeto la separación de documentos electrónicos siguiendo la clásica escisión del Código civil entre documento público y documento privado[595], y lo hace además en referencia a la forma de probar las obligaciones y la verificación de su autenticidad, con lo que su contenido, aunque perfectamente asumible por el Derecho penal, no aporta demasiado más que podamos añadir a lo ya enunciado. La idea fundamental en relación con el objeto

[591] Ver gráficamente las referencias al ámbito civil que se realizan constantemente en el Capítulo X de DAVARA RODRÍGUEZ, M.A.: *Manual…* ob.cit. pp. 437 a 495.

[592] DAVARA RODRÍGUEZ, M.A.: *Manual…* ob.cit. pp. 438 y ss., establece como tipos de documentos informáticos los *printout*, que son aquellos que se encuentran en un soporte físico (por ejemplo papel) que se han generado a partir de un medio informático; los *input*, que serán aquellos que se encuentran almacenados en un soporte informático; y finalmente los EDI (*Electronic Data Interchange*) "considerado como un soporte de información electrónico formado mediante el intercambio de mensajes con una estructura determinada".

[593] Nos referimos por ejemplo a un documento electrónico de texto que ha sido impreso en papel de tal forma que puede ser interpretado directamente por el ser humano. Excluimos por tanto aquella situación en la que un documento de texto, es grabado en un soporte físico como pueda ser una memoria USB, caso en cual seguiría constituyéndose como documento electrónico.

[594] MARCHENA GÓMEZ, M.: *Internet…* ob. cit. p. 361, con acierto reflexiona que "entre hacer trizas un documento […] o destruir ese mismo documento oprimiendo *delete*, no parece que pueda existir una diferencia cualitativa tan sustancial que se traduzca en un distinto tratamiento penal.

[595] El Código civil dedica a los documentos públicos los artículos 1216 al 1224 y los privados del 1225 al 1230 cuando se refiere a los modos de probar las obligaciones.

material del delito es, pues, que el tipo penal no protege el documento electrónico en sí, sino la integridad de la información contenida en ese documento electrónico.

Por último, el objeto material del delito en el caso del apartado segundo del artículo 264 CP es el "sistema informático", concepto donde también pueden surgir dudas, aunque menores, sobre lo que debemos entender por el mismo. El Convenio sobre la Ciberdelincuencia de Budapest de 2001 utiliza en su texto la expresión "sistema informático" que luego es sustituida en el texto de la Decisión Marco 2005/222/JAI de 24 de febrero por la de "sistemas de información", y que finalmente ha sido traspuesta a nuestro Código penal otra vez con la referencia a "sistemas informáticos". La cuestión que se plantea, aparte de la puramente terminológica, que según creemos es más acertada cuando utiliza la expresión "sistema informático"[596], es la relativa a las diferencias entre la definición ofrecida por el Convenio y la de la Decisión Marco[597]. Ambas son coincidentes en referirse a sistema informático (o de información) como un equipo o un grupo de equipos conectados entre sí que realizan (por lo menos uno de ellos) el tratamiento automático de datos informáticos gracias a programas. Es decir, que un sistema informático puede ser un solo equipo, siempre que tenga un *software* que realice el tratamiento de datos; o bien varios equipos que cumplan la misma descripción y que estén conectados entre ellos.

Hasta aquí parece no existir problema alguno, pero la definición de la Decisión Marco establece, a continuación, una fórmula cuando menos sorprendente,

[596] LAPIEDRA ALCAMÍ: *Diferencia…* ob. cit. (sin numerar), señala que "con la generalizada y amplia utilización de las tecnologías de la información se está llegando a confundir los conceptos de sistema de información y sistema informático. Sin embargo, el Sistema informático consiste en la compleja interconexión de numerosos componentes de *hardware* y *software*, los cuales son básicamente sistemas deterministas y formales, de tal forma que con un *input* determinado siempre se obtiene un mismo *output*. En cambio, los sistemas de información son sistemas sociales cuyo comportamiento se ve en gran medida influido por los objetivos, valores y creencias de individuos y grupos, así como por el desempeño de la tecnología. Así pues, el comportamiento del sistema de información no es determinista y no se ajusta a la representación de ningún modelo algorítmico formal."

[597] El convenio sobre la Ciberdelincuencia de Budapest de 2001 establece exclusivamente que por "sistema informático se entenderá todo dispositivo aislado o conjunto de dispositivos interconectados o relacionados entre sí, siempre que uno o varios de ellos permitan el tratamiento automatizado de datos en ejecución de un programa". La Decisión Marco 2005/222 JAI de 24 de febrero establece que se entenderá por sistema de información "todo aparato o grupo de aparatos interconectados o relacionados entre sí, uno o varios de los cuales realizan, mediante un programa, el tratamiento automático de datos informáticos". Fórmula que luego amplía con otros conceptos.

por compleja, cuyo significado no ha sido aclarado por la doctrina. Así, a la parte ya analizada se añade la fórmula: "[…] así como los datos informáticos almacenados, tratados, recuperados o transmitidos por estos últimos para su funcionamiento, utilización, protección y mantenimiento". Lo que, a nuestro juicio, pretende expresar la Decisión Marco, es que los datos informáticos, y no sólo los programas, son parte del sistema, y, además, los datos que se encuentran en tránsito entre sistemas informáticos también deben ser considerados dignos de protección, y por tanto los integra como parte del sistema informático. Esta interpretación se entiende desde el momento en que la expresión "por estos últimos" se refiere al equipo o grupo de equipos conectados entre sí, de tal forma que quiere expresar que los datos son parte íntegra, inseparable, del sistema informático. Son un todo con los propios equipos y los programas que tratan esos mismos datos. Esta matización que realiza la Decisión Marco, y que no aparece en el Convenio, no parecía necesaria por cuanto parece lógico que los datos informáticos y su tratamiento son al fin y al cabo la razón de existir de los sistemas informáticos y de los programas que los gestionan, de tal manera que no puede concebirse un sistema informático que funcione sin datos y, por tanto, los mismos ya estaban implícitamente protegidos con el mero hecho de proteger el sistema informático en general, existiendo, además, para su concreta defensa, el tipo penal correspondiente a los daños sobre datos, programas informáticos o documentos electrónicos.

4. ANÁLISIS DEL TIPO SUBJETIVO

A) TRATAMIENTO DEL DOLO EN LOS DAÑOS INFORMÁTICOS

a.1. El dolo en los delitos de daños informáticos.

El artículo 264 CP exige que se actúe con dolo en los tipos penales que recoge. Mucho se ha debatido en la doctrina sobre el concreto tipo de dolo que se requiere para poder considerar la conducta de daños clásicos como típica[598]. Extrayendo en síntesis esa discusión, se trata de entender si es necesario un dolo específico de dañar, que ha venido entendiéndose como la voluntad especial de

[598] La discusión doctrinal se presenta en SANTA CECILIA GARCÍA, F.: *Delito*… ob. cit. pp. 318 y ss. y ANDRÉS DOMÍNGUEZ, A.C.: *El Delito*… ob. cit. pp. 168 y ss.

perjudicar -*animus nocendi*- o por el contrario, no es necesario ese dolo específico y es suficiente el dolo (conocimiento y voluntad) de dañar el objeto -*animus damnandi*-. Lo cierto es que tal discusión puede extrapolarse sin duda a los daños informáticos, pero debe analizarse con atención cuando de estos delitos de nuevo cuño se trata. Esto ocurre así porque exigir un dolo específico de dañar en los delitos de daños informáticos, podría llevarnos a la impunidad de un importante número de situaciones que ponen en peligro el bien jurídico protegido. Es por lo tanto más adecuado a nuestro parecer entender la necesidad sólo de dolo general de dañar en nuestro caso también[599] y no el dolo concreto de perjudicar, porque de lo contrario, en los daños informáticos, la aparición del dolo directo de segundo grado, y especialmente del dolo eventual, quedarían excluidas en la mayoría de los casos, convirtiendo ciertas acciones comunes en este ámbito en atípicas por falta de apreciación del tipo subjetivo. Se puede pensar, por ejemplo, en esas situaciones en las que el sujeto activo simplemente lanza un virus por la red, o envía documentos infectados a una lista de correos electrónicos al azar; no parece complicado probar la existencia de un dolo general de dañar, pero supondría un esfuerzo adicional muy considerable el tener que probar un dolo concreto de perjudicar. Por ello, especialmente en los casos de delitos informáticos, y también opina así la doctrina mayoritaria para el resto de tipos de daños, es mejor entender el dolo solamente como el dolo genérico de dañar[600].

Por tanto, en cuanto la posibilidad de apreciar dolo directo de segundo grado y dolo eventual, la inexistencia de elementos en el tipo enunciados como "a sabiendas" o "intencionadamente" y lo ya referido en las líneas anteriores nos permite aceptar la posibilidad, sin excusas, de la aparición de estas dos modalidades de dolo. Así, nada impide que el dolo directo de segundo grado se produzca en casos

[599] CORCOY BIDASOLO, M.: "Problemática…" ob. cit. p. 27, "aun cuando no se exija que el sujeto conozca y quiera el resultado lesivo, para que una conducta pueda calificarse como dolosa el autor debe conocer el efectivo y exacto peligro que ésta supone. Sólo los resultados que sean realización de este peligro conocido por el sujeto pueden ser imputados a la conducta. Nos encontramos, por tanto, frente a supuestos que deberíamos calificar como *dolus generalis".* De la misma opinión GONZÁLEZ RUS, J. J.: "El cracking…" ob. cit. p. 247.

[600] ANDRÉS DOMÍNGUEZ, A.C.: *El Delito… ob. cit.* p. 169. Por su parte SANTA CECILIA GARCÍA, F.: *Delito*… ob. cit. p. 320, sentencia que "en todo caso, la anterior clasificación dolo genérico dolo específico, se encuentra superada por no responder a los modernos patrones dogmáticos y político criminales actuales".

en los que sin ser el objetivo directo de la acción, los resultados producidos son necesarios para completar la acción principal. Este sería el caso de aquel que con la intención de descubrir un secreto que se encuentra en un sistema informático, conoce que debe alterar unos datos del propio sistema y lo hace. Su objetivo no era causar el daño, pero sabe que su actuación lo supone de forma necesaria y lo acepta. Por otro lado, el caso del dolo eventual es igualmente posible en estos delitos, de hecho su aparición será frecuente en los casos en los que un sujeto lanza uno varios virus informáticos a la red, sin existir una víctima concreta hacia el que va dirigido, o incluso si desata una infección accidental al estar manipulando *software* malicioso. En estos casos, cuando ese virus cause daños informáticos en algún sistema en concreto, la aparición del dolo eventual resultará la única vía de imputación del resultado a la acción del atacante[601]. Otra situación relativa al dolo eventual sería aquella en la cual el atacante introduce un *software* malicioso con la intención de dañar un documento electrónico, pero finalmente no sólo se borra el archivo que se deseaba atacar, sino todos los demás documentos del equipo[602].

a.2. Elementos subjetivos del injusto.

Si bien no se advierte la presencia de elementos subjetivos del injusto en la redacción que se ha utilizado para tipificar los daños informáticos, alguna duda puede recaer sobre el elemento "de manera grave" entendido bajo el prisma que lo hicimos en páginas anteriores, como equivalente a "con el medio idóneo".

No existen en la doctrina ni en la jurisprudencia referencias sobre este extremo. La teoría general del delito establece que son elementos subjetivos del tipo "aquellos requisitos de carácter subjetivo distintos al dolo que el tipo exige, además de éste, para su realización"[603]. En nuestro caso sería el sujeto que quiere usar un medio determinado porque es el idóneo para conseguir el resultado para dañar que busca. No sólo se trata de que el medio sea idóneo, sino que el sujeto activo sabe que lo es y por ello lo utiliza. Aunque como hemos dicho, esta idea surge entre otros

[601] ORTS BERENGUER, E. y ROIG TORRES, M.: *Delitos…* ob. cit. p. 84.

[602] Supuesto en el que también podríamos encontrarnos ante una acción imprudente, DE LA MATA BARRANCO, N. J.: "El delito…" ob. cit. p. 171.

[603] MIR PUIG, S.: *Derecho…* ob. cit. pp. 278 y ss. y OCTAVIO DE TOLEDO Y UBIETO, E. y HUERTA TOCILDO, S.: *Derecho…* ob. cit. pp. 135 y ss.

motivos por la complicada interpretación para el término "de manera grave" que utiliza el Código, en principio parecería correcto no acudir al elemento subjetivo y limitarnos a analizar si la manera es grave únicamente atendiendo a si el medio es objetivamente el idóneo o no[604].

B) LA IMPRUDENCIA EN LOS DAÑOS INFORMÁTICOS

La modalidad imprudente en los delitos de daños informáticos viene recogida en el artículo 267 CP. Aunque, siendo estrictos, lo que tipifica este artículo es la imprudencia con carácter general en los delitos de daños, abarcando tanto los daños clásicos como los daños informáticos.

De esta idea podemos extraer que los elementos típicos en el caso de la imprudencia serán los ya analizados en el tipo objetivo para los dos tipos de daños informáticos, siendo el único cambio el del resultado, que pasa "de ser grave", con las dificultades ya puestas de manifiesto en su momento, a situarse en un perjuicio económico (en los mismo términos que los ya explicados, es decir el valor económico concreto de los datos, programas informáticos, documentos electrónicos dañados o los sistemas informáticos interrumpidos u obstaculizados; excluyendo otro tipo de perjuicios económicos) de ochenta mil euros. Resulta curioso que el legislador utilice una cifra concreta para subsumir un daño informático cuando se causa por imprudencia, y no lo haga cuando se hace con dolo. Esta situación se puede entender desde la perspectiva de que el delito de daños imprudentes tiene, en la concepción clásica, como delito doloso "asociado" el del artículo 263.1 CP referido a los daños clásicos que sí cuantifican el límite a partir del cual estamos ante el mismo, situación que como sabemos no ocurre en el nuevo artículo 264 CP relativo a daños informáticos.

Sobre este artículo, cabría añadir únicamente que parte de la doctrina entiende exagerada la sanción penal cuando se comete un daño informático de manera

[604] Aunque la todavía escasa doctrina no se ha manifestado excesivamente en este tipo de delitos, HUETE NOGUERAS, J.: "La reforma…" ob. cit. p. 3, plantea la vinculación entre la expresión "de manera grave" y la expresión "intencionadamente" que ocupaba su lugar en el texto de la Decisión Marco 2005/222/JAI de 24 de febrero del Consejo y que fue eliminada por el legislador español. Aceptar esta interpretación del significado de la gravedad en la forma de actuar, podría dar lugar a entender que sí nos encontramos ante un elemento subjetivo del injusto.

imprudente[605]. Cuestión que nos parece errónea, pues como se ha venido observando, la tipificación de las conductas del artículo 264 CP siempre ha tenido una penalidad mayor que las de los daños clásicos -ya era de esta manera con el antiguo 264.2 CP- lo que parece indicar el especial desvalor de estas conductas para el legislador; dicho lo cual, lo que sería incongruente sería sancionar las conductas imprudentes de unos daños que se consideran menos graves, y dejar impunes las conductas imprudentes de los daños considerados más graves.

En todo caso, a la vista de la diferente naturaleza entre los daños clásicos y los daños informáticos, también cabría preguntarse sobre lo idóneo de utilizar este artículo para perseguir delitos de daños informáticos imprudentes, y si no debería existir en realidad un artículo o un apartado concreto en el Código penal sobre los daños informáticos imprudentes. Especialmente en vista de que el principio de legalidad penal podría ser conculcado, e invocado por todos aquellos afectados, refiriendo que el daño informático imprudente no está realmente tipificado, siendo dicha pretensión, en nuestra opinión, nada descartable.

5. CIRCUNSTANCIAS MODIFICATIVAS QUE AFECTAN A LOS DAÑOS INFORMÁTICOS

A) AGRAVANTES GENÉRICAS Y SUPUESTOS AGRAVADOS

a.1. Agravantes genéricas del artículo 22 CP.

Sobre los delitos del artículo 264 CP puede producirse la aplicación de las agravantes comunes que están recogidas en el artículo 22 del Código penal. Entre ellas, la doctrina realiza una subdivisión entre aquellas que se consideran tienen un carácter objetivo, -"denotan mayor peligrosidad o suponen un ataque más extenso"-, y circunstancias de carácter subjetivo -basadas en la motivación o la actitud del sujeto-[606].

[605] DE LA MATA BARRANCO, N. J.: "El delito…" ob. cit. p. 172, señala que se puede considerar "desproporcionada o inadecuada la intervención penal en tales casos, considerando suficiente la reparación en sede civil".

[606] MIR PUIG, S.: *Derecho…* ob. cit. pp. 622 y ss.

Entre el primer grupo, tanto el abuso de superioridad, como el abuso de confianza y la circunstancia relativa al carácter público del culpable, parecen poder apreciarse sin demasiada dificultad. En efecto, el abuso de superioridad se producirá, por ejemplo, cuando aquel que realiza el ataque informático, teniendo amplios conocimientos en la materia, elige atacar datos o sistemas informáticos especialmente desprotegidos por no disponer de un sistema de seguridad eficiente o un equipo de administradores del sistema capaces de contrarrestar el ataque. El abuso de confianza será frecuente entre empleados y empleadores, en la medida que el empresario confía una serie de sistemas a un empleado y éste los utiliza oportunamente para cometer los hechos. Para terminar con este bloque, parece igualmente probable que el culpable pueda prevalerse de su carácter público para producir daños de esta índole. Aunque los ejemplos expuestos no agotan la extensísima casuística en la que pueden derivar los comportamientos humanos en la realización de estos delitos, basten como indicadores de que tales circunstancias agravantes son perfectamente aplicables a los delitos del artículo 264 CP.

En cuanto a la realización de los tipos por medio de disfraz, parece algo más complicado. Las técnicas destinadas a ocultar la identidad del atacante cuando nos referimos a ataques lógicos a los datos o los sistemas informáticos, a través de métodos tecnológicos o *software* malicioso, tendrían mejor encaje en la figura de la alevosía, sin embargo la configuración de la alevosía impide que pueda aparecer en la comisión de delitos contra la propiedad[607]. La alternativa ante esta situación sería subsumir este tipo de prácticas en las relativas al abuso de superioridad, pues ocultarse en la red tras cometer un delito de daños denota unos conocimientos específicos superiores a los habituales y parece una buena forma de procurarse la mejor perpetración del delito.

Las circunstancias relativas a aprovechamiento de lugar y el tiempo pueden igualmente suceder, en especial cuando el medio por el que se ataque a los datos,

[607] Artículo 22.1 CP: Ejecutar el hecho con alevosía. Hay alevosía cuando el culpable comete cualquiera de los delitos contra las personas empleando en la ejecución medios, modos o formas que tiendan directa o especialmente a asegurarla, sin el riesgo que para su persona pudiera proceder de la defensa por parte del ofendido. MIR PUIG, S.: *Derecho…* ob. cit. p. 625. "Tal vez sea conveniente mantener el criterio […] y, en consecuencia, limitar la agravante a los delitos contra las personas en su realidad física corporal.

programas informáticos o documentos electrónicos, o a los propios sistemas informáticos se realice a través de la actuación física sobre los soportes que los contienen (*hardware*). En el caso de los ataques lógicos, la apreciación de tales agravantes podría aparecer sólo en la relativa al tiempo, por ejemplo atacar cuando se conoce que se están llevando labores de mantenimiento de un servidor de seguridad y el sistema estará más desprotegido. El lugar, en el caso de ataques lógicos, sólo podrá ser el que ocupen los sistemas informáticos, por lo que no parece posible favorecerse de tal circunstancia. El aprovechamiento del auxilio de otras personas que debiliten la defensa del ofendido o faciliten la impunidad del delincuente, al igual que la alevosía, quedarían excluidas en estos delitos, pues se refieren a cuestiones relativas a la realidad física de las personas.

Las circunstancias agravantes subjetivas en relación con los tipos de daños informáticos tienen en común que son todas perfectamente aplicables a estos delitos. El precio, recompensa o promesa, los motivos racistas y discriminatorios y la reincidencia, dependen de las motivaciones y modos de actuar de los sujetos activos, y por tanto pueden concurrir en prácticamente todos los delitos del Código, siempre que no estén recogidos particularmente en otros tipos.

a.2. Supuestos agravados. El apartado tercero del artículo 264 CP.

Además de las posibles agravaciones genéricas comunes a todos los delitos de la parte especial, el apartado tercero del artículo 264 CP establece una serie de supuestos específicos en los que se endurece la pena de los tipos básicos en dos supuestos diferentes, no siendo necesaria la concurrencia de ambos, sino que basta la presencia de uno sólo para aplicar dicha agravación. La aparición de las mismas tienen directa relación con la correcta transposición de la Decisión Marco 2005/222/JAI de 24 de febrero[608], que determina en su artículo séptimo que los hechos relativos a la intromisión en sistemas informáticos y en datos se castigue con un marco penal abstracto cuyo límite inferior esté entre los 2 y los 5 años en los casos en que se cometan en el marco de una organización criminal[609]. Junto a esta

[608] MIRÓ LLINARES, F.: *Delitos…* ob. cit. p. 166.

[609] El artículo 7.1 de la Decisión Marco 2005/222/JAI de 24 de febrero establece que "cada Estado miembro adoptará las medidas necesarias para garantizar que las infracciones mencionadas en los

agravación se regula la posibilidad de que también se pueda señalar idéntico incremento de la penalidad -aunque no es imperativo en este caso- para las situaciones en las que se produzcan daños especialmente graves, o se afecte a intereses esenciales[610].

Volviendo a la regulación interna, el inciso primero del artículo 264.3 CP establece la agravación anterior en el caso de que los delitos de los apartados primero y segundo se hubiesen cometido en el marco de una organización criminal. La regulación de las organizaciones y grupos criminales se encuentra en el Código en los artículos 570 bis[611] y 570 ter. Por lo que respecta a nuestro precepto, sólo será aplicada la agravante cuando se actúe en el marco de organización criminal, no haciendo remisión expresa al grupo criminal. La previsión pues, para el caso de actuar en el marco de una organización criminal es que imponga la pena superior en grado, que sería de 2 a 3 años para el tipo del apartado primero, y de 3 años a 4 años y seis meses para el tipo del segundo apartado. Además de la pena de multa del tanto al decuplo del perjuicio ocasionado

Exactamente la misma penalidad se impondrá cuando concurra alguna de las dos posibilidades que se recogen en el inciso segundo del artículo 264.3 CP. Esto es, o bien que los daños ocasionados revistan especial gravedad, o bien que afecten a intereses generales[612]. Sobre el significado que utiliza el legislador cuando explicita la comisión de daños de especial gravedad se ciernen los mismos problemas que ya apuntamos a la hora de valorar lo que debía entenderse por un resultado grave como consecuencia de la realización de las acciones típicas. Sólo podemos afirmar que se

---

artículos 2, apartados 2, 3 y 4 se castiguen con sanciones penales de dos a cinco años de prisión como mínimo en su grado máximo cuando se cometan en el marco de una organización delictiva tal como la define la Acción Común 98/733/JAI, con independencia del nivel de sanción mencionado en dicha Acción Común."

[610] El artículo 7.2 de la Decisión Marco 2005/222/JAI de 24 de febrero establece que "los Estados miembros podrán adoptar asimismo las medidas contempladas en el apartado 1 cuando la infracción de que se trate haya ocasionado graves daños o afectado a intereses esenciales."

[611] El artículo señala que "a los efectos de este Código se entiende por organización criminal la agrupación formada por más de dos personas con carácter estable o por tiempo indefinido, que de manera concertada y coordinada se repartan diversas tareas o funciones con el fin de cometer delitos, así como de llevar a cabo la perpetración reiterada de faltas".

[612] Cabe destacar que se sustituya la expresión "intereses esenciales" de la regulación europea por la de "intereses generales" en la redacción del Código Penal.

trata de una gravedad todavía mayor a la de los tipos básicos[613]. Pero sin haber sido capaces de poner límite a la gravedad del tipo básico, se hace difícil poder establecerlo para el supuesto agravado. Menor indeterminación, aunque también patente, queda reflejada en el término de interés general, que no viene definido en el Código penal, y que la jurisprudencia ha tratado siempre en relación con cada precepto del Código, pero nunca como un concepto general[614].

No obstante, cabe interpretar esta fórmula cuando el daño pueda afectar no sólo al sujeto pasivo, sino a una pluralidad de personas; o bien, ligar el interés general al interés público y por tanto referir ese desvalor mayor a atacar instituciones propias del Estado. Lo cierto, como hemos señalado, es que este término deberá ser discutido por la doctrina y matizado por los tribunales cuando se enfrenten al mismo en relación con estos delitos.

a.3. Supuestos agravados. El apartado segundo del artículo 266 CP.

En el estudio relativo a los supuestos agravados no debemos olvidar las circunstancias de agravación comunes a todos los delitos de daños. En nuestro caso, el artículo 266.2 CP establece una penalidad de 3 a 5 años y multa de 12 a 24 meses para el que cometa los daños informáticos del artículo 264 CP mediante incendio, provocando explosiones o utilizando medios similares de potencia destructiva; o bien poniendo en peligro la vida o la integridad de las personas.

Estos supuestos de agravación tienen su origen en el riesgo especial que supone utilizar esos medios para cometer los hechos típicos. Lo cierto es que en los casos que estamos estudiando, la posibilidad de que tales situaciones se produzcan en la práctica puede existir -recordemos que el ataque físico como medio de conseguir un daño a datos, programas informáticos o documentos electrónicos era posible-. No obstante su apreciación en caso de ataques lógicos sería muy complicada, excepto en lo que se refiere a la puesta en peligro de la vida o la integridad de las personas, piénsese como ejemplo un ataque informático destinado a interrumpir los sistemas

[613] MIRÓ LLINARES, F.: *Delitos…* ob. cit. p. 167.

[614] STS 1136/2006 de 21 de diciembre en relación con un delito de información privilegiada; ATS de 17 de marzo 2009, en relación con un delito de calumnias; STS 88/1999 de 27 de enero, en relación con un delito de falsedades y STS 1030/2007 de 4 de diciembre, en relación con un delito de atentado contra autoridad pública y desobediencia, entre otras.

informáticos que gestionan la electricidad de un hospital. En tal caso, no cabe duda de que con el ataque realizado se pondría en juego la vida de los pacientes, por lo que tal agravante podría ser apreciada, más allá de otro tipo de delitos, además del daño informático, que por acción u omisión se pudiesen haber cometido. Quizá resulte aclaratorio el hecho de que el presente artículo no fue modificado con la entrada en vigor de la LO 5/2010 de 22 de junio, y pareciera que se estaba refiriendo especialmente a los daños agravados del artículo 263.2 CP que antes tenían sede en el artículo 264.1 CP -es decir, este artículo se concebía como una supuesto especialmente agravado de los daños clásicos-. Por tanto, se puede explicar que su previsión no parezca tener tanto encaje con el actual 264 CP, dedicado en exclusiva a los daños informáticos[615].

B) CIRCUNSTANCIAS QUE EXIMEN TOTAL O PARCIALMENTE DE RESPONSABILIDAD PENAL

b.1. Causas de justificación.

Para que se pueda constatar la prevalencia de un delito, además de afirmar que el hecho es típico por concurrir todos los elementos del tipo objetivo y el subjetivo, es necesario que tal comportamiento coincidente con el descrito en un tipo penal no se encuentre justificado por alguna causa que convierta la acción en antijurídica[616]. La legítima defensa, el estado de necesidad, el cumplimiento de un deber y ejercicio legítimo de un derecho, oficio o cargo son las causas de justificación que recoge el Código penal en su artículo 20.

[615] La Audiencia Nacional en Sentencia 5/2012 de 6 de febrero, señala la incongruencia entre las nuevas penas que se aplican a los daños cometidos mediante incendio y las aplicadas antes de la reforma, al haber sido ubicados dichos tipos penales en diferentes artículos del Código respecto de donde se encontraban anteriormente (llega a afirmar que "no descartamos que este efecto favorable al reo sea producto de un descuido del legislador"). Ello ha provocado ya la condena de un imputado a una pena de prisión considerablemente menor de lo que parece que el legislador preveía y el inicio de procesos de revisión de condena al resultar la situación actual favorable al reo respecto de la anterior, cuando de no haberse producido dicha reubicación el marco penal debería seguir siendo superior: el Tribunal explica que, en virtud de la reforma penal de 2010, la agravación por incendio del artículo 266.2 CP que se refería a los daños recogidos en el antiguo artículo 264.1 CP, debería haberse modificado, pasando ahora a referirse al artículo 263.2 CP, que es donde se sitúan tras la reforma los daños del antiguo 264.1 CP.

[616] OCTAVIO DE TOLEDO Y UBIETO, E. y HUERTA TOCILDO, S.: *Derecho*… ob. cit. p.157 o MIR PUIG, S.: *Derecho*… ob. cit. p. 421.

La configuración general de todas ellas encuentra acomodo en los delitos de daños informáticos del artículo 264 CP. Al igual que hicimos con las agravaciones generales del Código penal, baste aportar algunos ejemplos en los que se puede apreciar su presencia con facilidad. Un sistema informático está siendo atacado por un sujeto que ha conseguido acceder al sistema ajeno de manera remota, pero ese sistema cuenta con un administrador con los mismos o parecidos conocimientos informáticos, que verifica que la forma de evitar el ataque pueda ser transmitir una serie de datos informáticos que dañen el sistema atacante para así inutilizar su equipo y proteger el sistema propio. Tal acto de defensa sin duda supondrá un hecho típico del mismo tipo o análogo respecto del que realizaba el sujeto atacante, pero se encontrará justificado por la acción en legítima defensa. Por otro lado, las causas relativas al cumplimiento de un deber tendrán en la práctica más frecuencia y su estudio será menos complejo. Véase como ejemplo el policía que en cumplimiento de sus obligaciones interrumpe el sistema informático que hace de servidor de una página web de pornografía infantil.

La apreciación del estado de necesidad, tal y como se configura en nuestro ordenamiento, es sin duda la causa de justificación más problemática de encajar en estos supuestos. El peligro de un mal ajeno que lleva a la necesidad de lesionar un bien jurídico de otra persona en relación con la comisión de uno de los tipos del artículo 264 CP no parece tan sencillo de encontrar. El estado necesidad sitúa en peligro un bien jurídico, siendo lo verdaderamente importante "ante qué grado de peligro deben permitirse medidas salvadoras"[617]. Para valorar el conflicto se puede atender a diversas estimaciones: la comparación de los marcos penales, la diferencia de valor de los bienes jurídicos, la intensidad de la lesión del bien jurídico, el grado de los peligros que amenazan, el principio de autonomía, las regulaciones legales, la provocación -o no- del estado de necesidad, la existencia de deberes especiales, la actuación de parte del injusto, la importancia individual del daño evitado y del causado para los respectivos afectados o el origen del peligro en la esfera de la víctima de la injerencia[618]. Todo ello, como avanzamos, hace realmente complicado

[617] ROXIN, C.: *Derecho…* ob. cit. pp. 676 y ss.

[618] Son, en síntesis, todos los puntos a tener en cuenta para valorar la aparición del estado de necesidad según ROXIN, C.: *Derecho…* ob. cit. pp. 683 a 712.

poder afirmar o negar la existencia de tal circunstancia, pues su ponderación deberá supeditarse al caso concreto.

b.2. Causas de inimputabilidad.

Nuestro Código penal recoge además de las causas de justificación, otra serie de causas relacionadas con la culpabilidad, que de manifestarse producen la inimputabilidad de los sujetos activos. El ordenamiento jurídico exige dos requisitos para que pueda apreciarse la imputabilidad de un sujeto: que el sujeto tenga la capacidad de comprender lo ilícito y que tenga la capacidad de adecuar su comportamiento a esa comprensión[619]. Sentado esto, el Código penal recoge tradicionalmente como causas de inimputabilidad las de anomalía o alteración psíquica permanente, el trastorno mental transitorio, la minoría de edad y la alteración de la percepción.

Por lo que respecta a estas causas, dependen de la situación física y o mental del sujeto que realiza los hechos, de tal manera que no existe impedimento para que, en principio, pueda aparecer sobre el sujeto activo en los delitos de daños informáticos. Especial mención requiere la minoría de edad en cuanto a ataques de daños informáticos cometidos por medios lógicos y no físicos, pues es común que en una cantidad notable[620], los autores de estos hechos sean menores que tienen los conocimientos suficientes para realizarlos, lo que supone abrir un debate sobre lo especial de estos jóvenes delincuentes y el alcance de los hechos que cometen, pero que son juzgados con base en la Ley Orgánica 5/2000, de 12 de enero, reguladora de la responsabilidad penal de los menores e, incluso, en el caso de ser menores de 14 años, serán inimputables. Sobre este asunto, sería interesante profundizar en un estudio criminológico sobre el perfil del delincuente informático, para verificar sus características, y poder hacer así acertadas propuestas de política-criminal y de

[619] MIR PUIG, S.: *Derecho…* ob. cit. p. 565.

[620] Son muchas las noticias aparecidas en prensa sobre menores cometiendo estos delitos:
http://www.elmundo.es/elmundo/2009/11/26/navegante/1259238023.html
http://www.elmundo.es/navegante/2008/05/17/tecnologia/1211011772.html
http://www.elpais.com/articulo/Comunidad/Valenciana/Juicio/hackers/menores/edad/chantajear/companeros/elpepiespval/20090114elpval_2/Tes

reforma del Código penal y del menor, cuestión que excede del ámbito de la presente investigación[621].

b.3. El miedo insuperable.

Además, cabe mencionar igualmente el miedo insuperable, que no se configura como una causa de justificación ni de inimputabilidad, y sobre la que existen diferentes construcciones doctrinales[622], pero que tiene un efecto similar y es explicada comúnmente junto ellas[623]. En relación con la consumación de los hechos típicos a través de actos físicos sobre los sistemas informáticos que contienen los datos, programas informáticos o documentos electrónicos puede apreciarse en general la posible existencia de esta situación. En el caso de un ataque lógico para producir daños, puede contemplarse igualmente la situación, por ejemplo, de aquel que es impelido a realizar tal ataque bajo coacciones o amenazas.

b.4. Eximentes incompletas y atenuantes.

El artículo 21.1 CP establece que todas las causas que eximen de responsabilidad penal del artículo 20 CP, cuando no se den todos los requisitos que las configuran tendrán una incidencia atenuadora de la pena a imponer por los delitos que se hayan cometido. Dicho esto, baste señalar entonces que las mismas eximentes que pueden ser apreciadas en su forma completa para los delitos informáticos, van a poder ser apreciadas sin concurrir todos los requisitos, bien como eximentes incompletas, bien como atenuantes. Concretar tal cuestión deberá ser el papel de la jurisprudencia caso por caso.

---

[621] GALÁN MUÑOZ, A.: "Expansión…" ob. cit. p. 19, señala que "los estudios criminológicos nos demuestran que el delincuente informático es normalmente un sujeto que tiene unos conocimientos informáticos, respecto al funcionamiento del sistema del que abusa, no superiores al nivel de usuario y que, en líneas generales, no presenta especiales problemas de adaptación social". Someramente, sobre la responsabilidad penal del menor, véase REQUEJO NAVEROS, M. T.: "Criterios de determinación de la edad penal relevante. ¿A partir de qué momento el delito cometido por un menor merece la intervención penal?" en *Critica*, nº 976, 2011, pp. 26 y ss.

[622] Sobre la discusión centrada en si debe ser considerado una causa de no exigibilidad o bien una causa de exculpación, véase OCTAVIO DE TOLEDO Y UBIETO, E. y HUERTA TOCILDO, S.: *Derecho*… ob. cit. pp. 363 y ss.

[623] MIR PUIG, S.: *Derecho*... ob. cit. p. 598. Lo define como una "situación de no exigibilidad, porque se entiende que el Derecho no considera exigible a nadie resistir a una presión motivacional excepcional que el hombre medio no podría soportar".

Los siguientes párrafos de este artículo 21 CP tratan situaciones que supondrán una penalidad atenuada pero en menor medida que las anteriores. Entre ellas se encuentran la grave adicción, el estado pasional, la confesión de la infracción a las autoridades y la reparación del daño. En cuanto a las dos primeras, relativas al estado físico-mental del sujeto, cabe decir lo mismo que se señaló con respecto a las causas de justificación subjetivas, por el mismo motivo, son perfectamente apreciables en los delitos de daños informáticos. Las dos segundas, relativas a un momento posterior a la consumación de los hechos, igualmente pueden ser apreciables en cualquier situación. Por último, el artículo 21.7 CP, ante la posibilidad de otras situaciones que permiten atenuar la responsabilidad penal establece las llamadas atenuantes analógicas[624], cuya aparición en los delitos informáticos puede igualmente producirse.

b.5. El caso especial del artículo 268 CP. La excusa absolutoria.

Por último, no debemos olvidar la existencia del artículo 268 del Código penal, que viene a eximir de responsabilidad penal a una serie de sujetos que se encuentran en determinada situación con respecto del sujeto pasivo. En concreto los cónyuges no separados o en proceso de separación, los ascendientes y hermanos -por naturaleza o adopción- y lo afines en primer grado si existe convivencia. Todos ellos, como decimos, estarán exentos de responsabilidad criminal, siempre que los delitos patrimoniales no se hayan cometido mediando violencia o intimidación.

Aunque su estudio y debate excede del presente trabajo[625], el motivo de su existencia lo señala la Sentencia del Tribunal Supremo 334/2003 de 5 marzo en la que se señala que "la excusa absolutoria tiene su fundamento en incontestables

[624] MIR PUIG, S.: *Derecho…* ob. cit. p. 619.

[625] Para un tratamiento específico véase, QUINTERO OLIVARES, G.: *Comentarios a la Parte Especial del Derecho Penal*, Ed. Thomson Reuters, 9ª edición, Navarra, 2011, p. 766 y LOBO GONZÁLEZ, R. y ÁLVAREZ RODRÍGUEZ, M.: "Comentario al artículo 268 CP" en AMADEO GADEA, S. (dir.): *Código Penal. Doctrina Jurisprudencial. Parte especial,* Ed. Factum Libri Ediciones, Madrid, 2009.

parámetros de política criminal que desaconsejan la utilización de normas penales en las relaciones interfamiliares"[626].

6. PROBLEMAS CONCURSALES

A) CASUÍSTICA GENERAL

Son varias las cuestiones que se pueden plantear con respecto a los delitos del artículo 264 CP en relación con su aparición en concurso con otras figuras del Código penal. Es común que cuando se realizan los hechos delictivos correspondientes a los daños informáticos puedan aparecer junto con ellos otras figuras típicas, y no siempre produciendo la misma situación. La casuística puede determinar la aparición de un concurso real o ideal de delitos, o bien un concurso de leyes. A ello dedicaremos las siguientes líneas.

En cuanto a la posibilidad de que se produzca la vulneración de dos o más infracciones con la ejecución de un solo hecho no cabe duda de que tal como han quedado regulados los daños informáticos en nuestro Código penal se posibilita claramente la producción de tal situación entre los apartados primero y segundo del artículo 264 CP. Situemos la acción. Aquel que realiza una conducta de las señaladas en el párrafo primero, de manera grave y sin autorización por la que daña datos informáticos ajenos está cometiendo los hechos típicos del artículo 264.1 CP. Por otro lado, el artículo 264.2 CP castiga al que interrumpa u obstaculice -de manera y con resultado grave, sin autorización y sobre sistemas informáticos ajenos- un sistema informático a través del daño a datos informáticos. Se desprende de ello que

[626] La citada sentencia continua exponiendo que "recordemos que la razón de ser de la excusa absolutoria de los delitos contra la propiedad que no impliquen violencia ni intimidación entre los parientes incluidos en la excusa absolutoria del art. 268 del vigente Código Penal, equivalente al art. 564 del anterior Código Penal, se encuentra en una razón de política criminal que exige no criminalizar actos efectuados en el seno de grupos familiares unidos por fuertes lazos de sangre en los términos descritos en el art. 268 porque ello, sobre provocar una irrupción del sistema penal dentro del grupo familiar poco recomendable que perjudicaría la posible reconciliación familiar, estaría en contra de la filosofía que debe inspirar la actuación penal de mínima intervención y última ratio, siendo preferible desviar el tema a la jurisdicción civil que supone una intervención menos traumática y más proporcionada a la exclusiva afectación de intereses económicos como los únicos cuestionados, de ahí que se excluya los apoderamientos violentos o intimidatorios en los que quedan afectados valores superiores a los meramente económicos como son la vida, integridad física o psíquica, la libertad y seguridad".

para cometer el tipo penal del artículo 264.2 CP puede ser necesario previamente la comisión de una modalidad del injusto del artículo 264.1 CP. Ante tal situación, un mismo hecho puede ser subsumido, aparentemente, en dos tipos penales del Código diferentes, pues será un daño del artículo 264.1 CP y también un daño del artículo 264.2 CP, siendo que el sujeto activo ha realizado únicamente una única acción. Estamos aquí ante los supuestos en que un hecho acompaña normalmente a otro. El hecho primero -el daño informático- no tiene que ser necesariamente realizado para la aparición del tipo del apartado segundo (además de a través de un daño informático, se puede interrumpir u obstaculizar el sistema mediante la introducción o transmisión de datos informáticos), pero sí es habitual que lo acompañe. En todo caso el contenido desvalorativo del tipo penal del párrafo segundo colma el del primero. Para esta situación -como para todas las que se produce el concurso de leyes- el Código penal establece una serie de pautas de resolución de estas situaciones, siendo aquí lo idóneo sujetarse al principio de especialidad, pues el precepto del artículo 264.2 CP reproduce las características del 264.1 CP, añadiéndole además otras específicas. Se sancionará entonces por la conducta que resulte ser más específica, en este caso la del párrafo segundo en la que se subsume el desvalor de la primera.

Por otro lado, aunque algunas voces en la doctrina estiman que pueden concurrir situaciones que desemboquen en el concurso ideal en este delito, pues nada lo impide[627], como expondremos a continuación, creemos que será más común la aparición de un concurso real o medial.

La posibilidad de que una pluralidad de hechos de un sujeto constituya una pluralidad de delitos -concurso real- puede ocurrir en estos delitos de forma común. Un caso que podría considerase frecuente sería aquel en el que además de dañar un sistema informático, se sustraigan del mismo documentos con la intención de apropiárselos. En este caso, el Código penal sigue el principio de acumulación

[627] MIRÓ LLINARES, F.: *Delitos…* ob. cit. pp. 165 y 166, establece que será frecuente la aparición de un concurso ideal en las situaciones en las que para dañar un sistema, se acceda al mismo o bien, para alterar (dañar) un documento se produzca un descubrimiento de secretos.

material de la pena[628]. De la misma manera puede resultar habitual que para dañar un determinado documento electrónico se incurra en un descubrimiento de secretos. Debemos acudir a la idea de la unidad de acción desde el plano jurídico[629], atendiendo a los resultados producidos y las conductas típicas realizadas. Si entendemos que existe unidad de acción en la actuación del sujeto, deberemos entonces acudir al concurso ideal, si por el contrario, como es nuestra opinión para la mayor parte de estos casos, no existe unidad de acción, sino que una cosa es la actuación que lleva al sujeto a cometer el daño informático y otra la actuación que lleva al sujeto a cometer el otro delito (apropiación de documentos, descubrimiento de secretos, etc.), entonces estaremos ante un concurso real -o medial-.

El problema de las conductas que ahora analizamos, es que puede ser difícil separar estas "unidades de acción" en situaciones diferenciadas, pues todo el proceso transcurre en muy breve espacio de tiempo y la acción de unos tipos se entremezcla con las de los otros, no son conductas lineales, sino entremezcladas entre sí. Por ejemplo, un sujeto accede ilegítimamente a un sistema informático vulnerando las medidas de seguridad para, a continuación, apropiarse de documentos electrónicos que se reenvía a su correo y finalmente introduce un virus que daña el sistema en su conjunto, todo ello mientras los administradores del sistema vulnerado intentan evitar estas acciones. La cuestión gira en torno a si el sujeto activo ha realizado una o varias acciones, pues en realidad se ha limitado a estar delante de un ordenador y teclear una serie de comandos. A nuestro juicio, a pesar de que físicamente el autor sólo realice una acción, creemos adecuado entender que realmente se han producido una serie de acciones diferenciadas (en el ejemplo propuesto al menos tres), que producen varios resultados, debiéndose aplicar el concurso real, y no el ideal.

Por último, además del concurso ideal y el real, nos parece importante detenernos en el concurso medial, que la doctrina tiende a subsumir como un tipo de

[628] Señalada en el artículo 73 CP, imponiendo la acumulación jurídica como límite en el artículo 76 CP, MIR PUIG, S.: *Derecho…* ob. cit. pp. 650 y 651, la acumulación material supone sumar las penas de los diferentes delitos. La acumulación jurídica supone imponer una pena más grave que la del delito más grave cometido, pero inferior a la que resultaría de sumar todas las penas de cada delito cometido.

[629] GIL GIL, A.: "Unidad y pluralidad de delitos" en GIL GIL, A.; LACRUZ LÓPEZ, J, M.; MELENDO PARDOS, M. y NÚÑEZ FERNÁNDEZ, J.: *Curso de Derecho penal. Parte General*, Ed. Dykinson, Madrid, 2011, pp. 713 y ss.

concurso real[630], y el Código lo sanciona el su artículo 77 equiparándolo al concurso ideal[631]. No cabe duda de que será uno de los protagonistas en la esfera de los delitos informáticos en general. Uno de los métodos válidos y que se realizan en la práctica real para consumar el delito de daños informáticos que hemos estudiado es conseguirse introducir, virtualmente, en los sistemas informáticos ajenos que se pretenden dañar, de tal forma que la figura del artículo 197.3 CP[632] va a cobrar especial relevancia en todo lo que concierne al concurso medial cuando de figuras relacionadas con la informática se refiere. En el caso que nos interesa, como decíamos, será habitual la aparición de este delito del artículo 197.3 del Código penal para, una vez hayamos accedido a ese sistema informático, conseguir dañarlo[633]. Cuando esta situación se produce, no parece haber problemas para apreciar la figura del concurso medial, en cuyo caso la conducta será sancionada por la pena superior en grado a la indicada para el delito más grave.

B) PLURALIDAD DE AFECTADOS Y DELITO CONTINUADO

Respecto a la naturaleza de las acciones de daños informáticos cabe la posibilidad de que un sujeto pueda cometer con una sola acción física múltiples resultados iguales (o esencialmente iguales[634]). En primer lugar cabría preguntarse sobre si el sujeto activo ha realizado una acción o varias. Debe responderse, desde una óptica informática, que el ataque informático sobre diferentes sistemas de información, aunque puede constar de una solo acción física (por ejemplo introducir en un e-mail un archivo que va a destruir datos en los sistemas informáticos de los sujetos que lo reciben; y enviarlo a una pluralidad de personas) es en realidad, y

[630] MIR PUIG, S.: *Derecho…* ob. cit. pp. 648 y ss.

[631] GIL GIL, A.: "Unidad…" ob. cit. p. 724.

[632] Artículo 197.3 CP: "El que por cualquier medio o procedimiento y vulnerando las medidas de seguridad establecidas para impedirlo, acceda sin autorización a datos o programas informáticos contenidos en un sistema informático o en parte del mismo o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho a excluirlo, será castigado con pena de prisión de seis meses a dos años".

[633] Es, por ejemplo, una acción diferente a la de enviar un correo electrónico con un virus. En ese caso el atacante no accede a los datos ni al sistema informático ajeno. Se puede decir que lo daña en la distancia.

[634] El atacante que envía a varias víctimas un fichero infectado que borra sus fotos, produce el mismo resultado en todos los sistemas atacados, esto es la desaparición de sus fotografías, independientemente de que la cantidad de fotografías que tuviesen unas u otras víctimas.

como hemos señalado en relación a los concursos, una pluralidad de acciones típicas, si bien éstas de la misma naturaleza.

Sentada dicha apreciación, cabría entonces señalar si nos encontramos ante un delito continuado del artículo 74.1 CP o más específicamente ante un delito masa del artículo 74.2 CP, interrogante que se debe resolver en favor de la segunda opción, básicamente por encontrarnos en todo caso, y como así ha decidido el legislador a la hora de ubicar los delitos de daños informáticos, dentro de delitos patrimoniales, que se guiarán por lo establecido en el artículo 74.2 CP[635]. Pero es que además, las características del ejemplo antes propuesto se acomodan con naturalidad a los criterios de distinción propuestos por la doctrina para el delito masa, como son la indeterminación del sujeto pasivo, confeccionado como una colectividad de personas indeterminadas, y que la pluralidad de acciones no precise de sucesión gradual entre ellas[636].

De esta forma, se contempla una penalidad que puede llegar a ser sustancialmente mayor, pudiendo llegar a aumentar el marco penal abstracto hasta dos grados.

7. CONSECUENCIAS JURÍDICAS

A) REFERENCIA A LOS MARCOS INTERNACIONALES

Al analizar la penalidad de las conductas que hemos desarrollado en los apartados anteriores no debemos olvidar que su origen se encuentra en la regulación internacional de la materia, por lo que es obligado el estudio de estas normas

[635] Refiriéndose al delito masa del artículo 74.2 CP como un subconjunto del delito continuado, CORCOY BIDASOLO, M.: "Problemática…" ob. cit. p.30, señala que "la multiplicidad de resultados lesivos imputables a una única conducta plantea la cuestión concursal. Es necesario delimitar cuándo nos encontramos frente a un concurso ideal o real de delitos o, en su caso, frente a un delito continuado. Parece claro que en aquellos delitos que afectan al patrimonio, en sus distintas versiones, estafas, sabotaje informático…, lo adecuado sea aplicar la figura del delito continuado". También VELASCO NÚÑEZ, E.: "Aspectos…" ob. cit. pp. 2 y 3 o ROMEO CASABONA, C. M: "De los delitos…" ob. cit. p. 27 y NÚÑEZ FERNÁNDEZ, J.: "Aplicación y determinación de la pena" en GIL GIL, A.; LACRUZ LÓPEZ, J, M.; MELENDO PARDOS, M. y NÚÑEZ FERNÁNDEZ, J.: *Curso de Derecho penal. Parte General*, Ed. Dykinson, Madrid, 2011, p. 870.

[636] CHOCLÁN MONTALVO, J. A.: *El delito continuado*, Ed. Marcial Pons, 1ª edición, Madrid, 1997, pp. 369 y ss.

supranacionales en cuanto a sus imposiciones a los Estados en materia de penalidad aplicable.

La primera aproximación al establecimiento de un marco penal lo ofrece el Convenio sobre la Ciberdelincuencia de Budapest de 2001, en el que para las conductas que son de nuestro interés se establece que deben ser penadas a través de una fórmula tan amplia que renuncia a establecer marcos concretos: "cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para que los delitos previstos de conformidad con los artículos 2 a 11 puedan dar lugar a la aplicación de sanciones efectivas, proporcionadas y disuasorias, incluidas penas privativas de libertad"[637]. Es decir, la única conclusión que se extrae del mismo es la de que en todo caso la sanción por tales conductas deberá ser penal, y no de otro ámbito jurisdiccional. En cuanto a las personas jurídicas, su amplitud es todavía mayor, pues establece con la misma fórmula que las sanciones serán de carácter "penal o no penal". Es decir, para las personas jurídicas ni siquiera establece la obligatoriedad de la sanción penal por dichas acciones, sino simplemente que exista sanción[638]. La justificación parece encontrarse en la no existencia de responsabilidad penal de las personas jurídicas en todos los ordenamiento jurídicos -así era el caso del ordenamiento penal en el momento de la elaboración del Convenio-, de tal forma que con esta fórmula se salvaba dicho conflicto y se abría el marco para la adhesión de un mayor número de Estados.

Heredera del contenido del Convenio es la Decisión Marco 2005/222/JAI de 24 de febrero. En su artículo 6.2 establece ya un marco concreto de sanción para las conductas de intromisión ilegal en datos e intromisión ilegal en sistemas de información (lo que tras su trasposición es nuestro artículo 264 CP, apartado primero y segundo). Exige a los Estados miembros que para tales acciones las sanciones sean de uno a tres años de prisión como mínimo en su grado máximo[639]. La Decisión

[637] Artículo 13.1 (sanciones y medidas) del Convenio sobre la Ciberdelincuencia de Budapest de 2001.

[638] Artículo 13.2 (sanciones y medidas) del Convenio sobre la Ciberdelincuencia de Budapest de 2001.

[639] Artículo 6.2 (sanciones) de la Decisión Marco 2005/222/JAI de 24 de febrero. Esta expresión no se encuentra exenta de problemas, aunque de la lectura de la Decisión en otros idiomas parece

Marco en su artículo 9 establece las sanciones para las personas jurídicas que cometan los hechos descritos en los artículos anteriores. En concreto para los hechos que nos conciernen, aunque se impone la necesidad de sancionar, no se establecen sanciones concretas, e igual que el Convenio, no establece la obligación de la sanción penal, pudiendo aplicarse sanciones de carácter administrativo. Recoge un catálogo de posibles formas de reproche, además de las pecuniarias como son la exclusión del disfrute de ventajas o ayudas públicas, la prohibición temporal o permanente del desempeño de actividades comerciales, la vigilancia judicial, o medidas judiciales de liquidación[640].

B) LA PENALIDAD PREVISTA EN EL CÓDIGO PENAL

Volviendo ahora a nuestro ordenamiento interno, nos encontramos como resultado de las exigencias internacionales la necesidad de imponer para los tipos descritos, en el caso de personas físicas un marco mínimo de 1 a 3 años en su grado máximo, y con sanciones penales o administrativas en el caso de que el delito sea cometido por las personas jurídicas. Además, el supuesto de la penalidad de la comisión imprudente del tipo, que trataremos al finalizar este apartado, no viene marcado por imperativo internacional.

El primer punto en el que debemos detener el análisis es en lo que el legislador internacional ha querido expresar con la utilización de las fórmulas "marco mínimo en su grado máximo", pues es un asunto en el que la doctrina no se ha detenido y suscita dudas. Lo primero que se puede remarcar es que la redacción de la Decisión Marco de 2005 en todos los idiomas de la Unión Europea sigue dicha formulación. En cambio ésta no se corresponde con la formulación de marcos penales abstractos de nuestro ordenamiento, que nuestra doctrina ha desarrollado en torno a las ideas de límite máximo y límite mínimo de las penas correspondientes a cada delito. Por ello, a la hora de saber cómo transponer la norma europea debemos conocer a que se refiere exactamente. En primer lugar parece lógico descartar que la

deducirse que se refiere a que el límite superior, debe situarse entre 1 y 3 años, dejando a los Estados la delimitación que crean oportuna para el límite inferior. En todo caso, la redacción de la Decisión es manifiestamente mejorable.

[640] Artículo 9 (sanciones aplicables a personas jurídicas) de la Decisión Marco 2005/222/JAI de 24 de febrero.

norma esté estableciendo los límites máximo y mínimo de la penas a imponer, pues habla sólo de grado máximo. De ello cabe deducir que lo que pretende establecer es el límite máximo, y que éste deberá situarse entre el año y los tres años, dejando un amplio margen a los legisladores nacionales de establecer el límite máximo en sus regulaciones, así como un margen absoluto para determinar el límite mínimo, pues respecto del mismo no se hace referencia.

La penalidad del artículo 264.1 CP queda establecida según nuestro Código penal entre seis meses y dos años en su tipo básico. En este caso, el legislador ha optado por fijar el límite inferior -de exclusiva decisión nacional- en 6 meses, límite inferior al que se establecía en la anterior regulación (1 año) y ha fijado el límite superior en 2 años, un punto intermedio entre el máximo y el mínimo marcado en la norma internacional. La penalidad del artículo 264.2 CP a diferencia de la del apartado anterior es mayor, y queda comprendida entre los seis meses y los tres años. En este caso el legislador nacional ha llevado hasta el límite el requisito del marco superior de tres años planteado por la normativa europea, y ha decidido mantener el límite inferior en 6 meses. Para ambos tipos, en caso de concurrir alguna de las agravantes del apartado tercero del artículo 264 del Código penal, se impondrá su correspondiente pena en grado superior además de multa del tanto al decuplo del perjuicio ocasionado.

A mayor abundamiento el legislador español ha decidido libremente -pues no era imposición internacional- que las personas jurídicas que cometan los delitos de los apartados primero y segundo del artículo 264 del Código penal tengan responsabilidad penal (y no administrativa, como era posible también en aplicación de la Decisión Marco) con unas penas que son de multa del doble al triple del perjuicio causado en el caso de subsumirse la acción bajo los hechos del artículo 264.1 Código penal y del doble al cuádruple para el resto de casos. Además, se completa el catálogo de penas a las personas jurídicas estableciendo la posibilidad de imponer las sanciones generales contenidas en el artículo 33.7, letras b) a g) del Código penal[641], situándose entre ellas las que exige también la Decisión Marco.

[641] Artículo 33.7 CP: Las penas aplicables a las personas jurídicas, que tienen todas la consideración de graves, son las siguientes: a) Multa por cuotas o proporcional, b) disolución de la

Por último, en el caso del artículo 267 del Código penal relativo a la comisión de los daños de forma imprudente, el legislador, que no ha modificado el artículo con la última reforma, mantiene la pena de multa de tres a nueve meses en función de la importancia de los daños. Se recoge igualmente la posibilidad en esta comisión imprudente de la figura del perdón del ofendido, que extinguirá la acción penal.

C) LA FALTA DE DAÑOS DEL ARTÍCULO 625.1 CP

No se ha tratado hasta ahora la cuestión de la falta de daños regulada en el Código penal en el artículo 625.1, en la cual se castiga al que cometa daños (sin especificar de qué tipo) intencionadamente por un valor inferior a 400 euros. No hay duda de su conexión directa con el delito del artículo 263.1 CP de daños clásicos. Pero existen motivos suficientes para pensar que no pueda ser aplicado también a los daños informáticos cuando estos no sean graves como exige el tipo.

No se sabe si existe, en principio, alguna imposibilidad, por cuanto tal como se encuentra redactado, el tipo se refiere sin más a daños, lo que puede entenderse como referido a todos los tipos de daños que se regulan en Capítulo IX, del Título XIII del Libro II, "De los daños". Lo cierto es que aceptar está inclusión, pasa por plantearnos entonces, si todo daño informático de un valor hipotético inferior a 400 euros no será grave y deberá subsumirse en este tipo de falta, lo que a la postre llevaría a definir como daños informáticos graves aquellos cuyo valor es superior a 400 euros, y es patente que el legislador expresamente no ha querido regular ese límite. Se produce, por tanto, una incongruencia en la vinculación falta-delito, cuyo origen es anterior a la reforma penal de 2010 -pues ya se manifestaban dudas sobre si

---

persona jurídica. La disolución producirá la pérdida definitiva de su personalidad jurídica, así como la de su capacidad de actuar de cualquier modo en el tráfico jurídico, o llevar a cabo cualquier clase de actividad, aunque sea lícita, c) suspensión de sus actividades por un plazo que no podrá exceder de cinco años, d) clausura de sus locales y establecimientos por un plazo que no podrá exceder de cinco años, e) prohibición de realizar en el futuro las actividades en cuyo ejercicio se haya cometido, favorecido o encubierto el delito. Esta prohibición podrá ser temporal o definitiva. Si fuere temporal, el plazo no podrá exceder de quince años, f) inhabilitación para obtener subvenciones y ayudas públicas, para contratar con el sector público y para gozar de beneficios e incentivos fiscales o de la Seguridad Social, por un plazo que no podrá exceder de quince años y g) intervención judicial para salvaguardar los derechos de los trabajadores o de los acreedores por el tiempo que se estime necesario, que no podrá exceder de cinco años. […].Para un estudio en detalle, véase ZUGALDÍA ESPINAR, J. M.: *La responsabilidad*… ob. cit. pp. 131 y ss. y BACIGALUPO SAGGESE, S.: "Los criterios…" ob. cit. pp. 5 y ss.

el límite de los 400 euros era un requisito del anterior artículo 264.2 CP- pero que adquiere una especial significación con la redacción actual.

Otra cuestión relevante es si se puede interpretar que debe aplicarse este precepto no sólo cuando el daño informático sea inferior a 400 euros, es decir, no vincularlo en exclusiva al resultado y sí a la falta de alguno de los requisitos de conducta que exigen los tipos penales de los artículos 264.1 y 264.2 CP. Al fin y al cabo, el tipo de la falta del artículo 625.1 CP sólo exige un daño intencionado de un importe inferior a 400 euros, no requiriendo, por tanto, que la "manera sea grave", o que se lleve a cabo a través de una determinada conducta, extremos que como ya analizamos tienen un significado concreto y que ahora no son exigidas.

Vista esta abundante problemática para reconocer en el artículo 625.1 CP una supuesta falta de daños informáticos, nuestra posición es escéptica con respecto a la aplicabilidad de esta figura en el caso de que se produzcan daños informáticos de poca gravedad. Lo cual tampoco permite dar por finalizado el problema totalmente, pues no parece lógico que en los daños clásicos, en teoría de menor gravedad que los daños informáticos, se sancionen los casos menos graves a través de un precepto penal como es la falta, y los daños informáticos leves -en principio de mayor gravedad que los daños tradicionales leves- por el contrario, no merezcan protección penal alguna; o acaso se deba interpretar que todo daño informático, por tener dicha naturaleza, es grave *per se*, cuestión que tampoco parece acertada.

Por lo demás, la penalidad de este artículo es de localización permanente de dos a doce días o multa del diez a veinte días, aunque, como hemos expresado, no nos parece posible su aplicación en el caso de daños informáticos que no sean graves, que resultarían atípicos.

TERCERA PARTE:

EVALUACIÓN DE LA ACTUAL REGULACIÓN DE DAÑOS INFORMÁTICOS Y DELITOS CONEXOS. PROPOSICIÓN DE UN MARCO LEGISLATIVO ALTERNATIVO

CAPÍTULO CUARTO: DUDAS QUE SUSCITA LA ACTUAL REGULACIÓN. CONSTRUCCIÓN DE UN BIEN JURÍDICO AUTÓNOMO: LA SEGURIDAD EN LOS SISTEMAS DE INFORMACIÓN

1. INTRODUCCIÓN

Con este cuarto capítulo se da inicio a la tercera y última parte de la investigación sobre delincuencia y daños informáticos. Una vez hemos introducido la informática como ciencia, y la regulación general que de los daños informáticos se hace desde la perspectiva de la normativa internacional, y finalmente la realidad normativa española al respecto, es el momento de plantear, desde una posición prudente, algunos problemas o dudas que han surgido al hilo de la presente investigación. Así, van a ser analizados, desde diversas perspectivas, los problemas suscitados por la actual regulación penal de los daños informáticos. En efecto, del fenómeno de los daños informáticos surgen dudas en diferentes ámbitos: desde el ya repetido de la trasnacionalidad de las conductas y los problemas que de ello se derivan, pasando por otros relacionados con la forma de comisión del delito y la necesidad de las autoridades nacionales e internacionales de disponer de unos medios y conocimientos técnicos suficientes para perseguir estos delitos. Todo ello sin olvidar los problemas que de la tipificación de nuestro Código se pueden derivar, tanto su ubicación en el texto penal como los requisitos de los tipos penales de los daños informáticos, tal y como están expresados, pueden deparar problemas de interpretación.

Precisamente, en consonancia con estas cuestiones, se hará una reflexión sobre la idoneidad de la ubicación de los daños informáticos en el Código penal, afrontando si la misma es la más adecuada tal y como se regulan las conductas en el ámbito internacional y si, por tanto, protegen los bienes jurídicos para cuya defensa han sido introducidos. Todo ello nos llevará al último apartado de este capítulo, en el

que trataremos de establecer un nuevo bien jurídico merecedor de protección penal, que pueda resolver las dudas planteadas por la actual regulación.

2. CONFLICTOS DERIVADOS DE LA PERSECUCIÓN DE LAS ACCIONES DELICTIVAS

Aunque el ámbito de nuestra investigación se ve superado cuando tratamos de la persecución de los delitos de daños informáticos -u otros delitos relacionados con la informática- debido a lo multidisciplinar de éstos, cabe al menos realizar una serie de anotaciones respecto a uno de los singulares problemas que afecta a este tipo de conductas delictivas, que no es sino su persecución, tanto en el ámbito policial, como en el ámbito jurisdiccional.

Tal y como se encuentran tipificados el artículo 264 CP y otros delitos informáticos, y como ya se ha puesto de manifiesto al analizar los sujetos activos de estos delitos, nos encontramos ante un delito que puede ser cometido por cualesquiera sujetos, tanto personas físicas con o sin conocimientos sobre informática[642], como personas jurídicas.

Por lo que respecta a las personas físicas, debemos realizar una distinción básica, pues mientras aquellos daños informáticos producidos físicamente, esto es, destruyendo materialmente los dispositivos donde se encuentran los datos, programas informáticos o documentos electrónicos, no suponen una forma de comisión que presente problemas en cuanto a su perseguibilidad[643], no ocurre lo mismo cuando los

[642] DÍAZ GÓMEZ, A.: "El delito…" ob. cit. 174, señala sobre la delincuencia informática en general, aunque puede aplicarse a los tipos penales estudiados, que "cometer delitos informáticos es mucho más sencillo de lo que pudiera parecer. En primer lugar requieren escasos recursos por parte del delincuente (apenas un ordenador conectado a la Red) y como se ha visto, pueden asimismo cometerse desde cualquier lugar del mundo. Pero además puede ser extremadamente sencillo hacerlo, hasta el punto que una persona con escasos conocimientos de informática sería hipotéticamente capaz de lograrlo. Aún digo más, puede llegar a hacerlo sin siquiera ser muy consciente de ello. Lógicamente, en este punto conviene diferenciar entre los distintos tipos delictivos, puesto que salta a la vista que las grandes estafas informáticas o la creación de complejos programas destructores no pueden ser llevadas a cabo por personas con limitado conocimiento de sistemas informáticos".

[643] Ya se ha señalado en esta investigación, que mientras exista dolo de destruir los datos, programas informáticos o documentos electrónicos por parte del sujeto que destruye físicamente el sistema informático donde estos se encuentran, además de los daños clásicos, resultará una relación concursal con la comisión de unos daños informáticos.

daños informáticos son cometidos por medios informáticos, y mucho menos cuando los daños son cometidos de forma remota a través de redes de comunicaciones (Internet). En resumen, los daños informáticos del artículo 264 CP pueden ser realizados por tres vías: a) medios físicos, b) medios informáticos de forma presencial o eminentemente presencial, c) medios informáticos de forma remota. Siendo la forma segunda y tercera, y muy especialmente la tercera, las que plantean los mayores problemas de persecución y sobre las que nos detendremos en las siguientes líneas[644].

A) EN EL ÁMBITO POLICIAL

Las instituciones internacionales siempre han manifestado su preocupación por la capacidad que tienen los ataques informáticos de afectar al normal desarrollo de la sociedad[645], y en los últimos años, especialmente en el seno de la Unión Europea, se han venido aprobando resoluciones para desarrollar una organización conjunta dirigida a proteger las infraestructuras de la información de ataques informáticos externos[646]. En este contexto, la palabra externo adquiere un doble significado. Por un lado, externo como realizado por sujetos ajenos a los Estados (que no descarta que puedan ser cometidos por sujetos vinculados al Estado, sino simplemente que no diferencia la situación de otras amenazas comunes) y, por otro lado, y más importante, externos en el sentido de ser realizados en la distancia, ya que es este extremo el que dificulta la persecución de tales acciones[647].

---

[644] Lo expresa claramente VELASCO NÚÑEZ, E.: "Aspectos…" ob. cit. p. 6, cuando señala que "si hay alguna característica singular de la delincuencia informática, más que la de su sofisticación tecnológica, es la de que el infractor suele ser un delincuente cobarde, que tira la piedra y esconde la mano, actuando casi sin riesgo y a distancia." También se refiere a ello MORENÉS ÁLVAREZ DE EULATE, P.: "Nuevas tecnologías y seguridad. El tratado de Budapest, un paso más" en *Economista*, nº 91, 2002, p. 377, al definir el lugar de los hechos criminales como "espacio virtual", aun cuando los sujetos que los cometen "son reales".

[645] Se puede observar tanto en el Preámbulo del Convenio sobre la Ciberdelincuencia de 2001 como en el de la Decisión Marco de 2005.

[646] Ya nos hemos referidos a ellas en esta investigación: COM(2010)517 final, de 30 de septiembre de 2010, COM(2008)448 final, de 14 de julio de 2008, La COM (2007) 267 final, de 22 de mayo de 2007, COM(2001)298 final, Bruselas, 6 de junio de 2001, COM (2000) 890 final, de 26 de enero de 2001.

[647] CÁRDENAS ARAVENA, C. M.: "El lugar de comisión de los denominados ciberdelitos" en *Política Criminal: Revista Electrónica Semestral de Políticas Públicas en Materias Penales*, nº 6,

En efecto, los ataques informáticos, ya sean daños informáticos u otro tipo de actividades delictivas relacionadas con los sistemas de información, poseen la característica de poder realizarse remotamente, de tal manera que el primer problema que se plantea a la hora de determinar la naturaleza del ataque es su origen[648], cuestión primordial para iniciar la persecución del mismo y que no siempre es fácil de identificar[649], en primer lugar, porque existen medios técnicos informáticos para ocultar el rastro dejado por el atacante[650] y, en segundo lugar, porque en muchas ocasiones, especialmente en los ataques DDoS, no se trata de localizar al atacante inmediato, que suele ser una pluralidad de sujetos que en muchas ocasiones ni siquiera serán conscientes de estar participando en un ataque, sino de encontrar al organizador de dicho ataque, que puede no estar participando directamente en el mismo. Una vez resuelto este problema sobre la localización del origen del ataque, que no es menor y requiere a menudo de la actuación conjunta de Fuerzas y Cuerpos de Seguridad de varios Estados y de la utilización de medios técnicos adecuados y personal especializado[651], así como de la utilización de métodos de investigación

---

2008, p. 5, plantea de forma novedosa (aunque finalmente descarta) la posibilidad de que el lugar de comisión de los delitos, de hecho, no sea un Estado, sino el propio ciberespacio: "si bien es cierto que la materia que nos ocupa hoy se caracteriza marcadamente por la ausencia de fronteras físicas, no es menos cierto para los efectos de determinar el derecho aplicable y los tribunales competentes hemos de procurar subsumir esta manifestación cultural en la normativa vigente, pues ese es el fin de que se trate de normas generales y abstractas. Lo contrario sería asumir que ciertas conductas delictivas quedan fuera de la jurisdicción de cualquier Estado, lo que no parece defendible. Por lo tanto, se prescindirá en lo sucesivo de la alternativa de considerar el ciberespacio como lugar de comisión." También se refiere a este extremo RODRÍGUEZ BERNAL, A.: "España: los Cibercrímenes…" ob. cit. pp. 9 y ss.

[648] Desde la perspectiva jurídica, MAGRO SERVET, V.: "La delincuencia…" ob. cit. (edición electrónica sin numerar), manifiesta en este sentido que "la mayor dificultad de la persecución de la delincuencia en Internet se centra en la localización de la autoría del hecho, aparte de los problemas ya mencionados de la extraterritorialidad y la necesidad de una gran cooperación internacional bajo la idea de un Código común". También expresado por las Fuerzas y Cuerpos de Seguridad del Estado en SALOM CLOTET, J.: "Delito informático y su investigación" en VELASCO NÚÑEZ, E. (dir.): *Delitos contra y a través de las nuevas tecnologías. ¿Cómo reducir su impunidad?*, Ed. Consejo General del Poder Judicial, Cuadernos de Derecho Judicial, 1ª edición, Madrid, 2006, pp. 123 y 124 y FERNÁNDEZ LÁZARO, F.: "La Brigada…" ob. cit. pp. 134 y ss.

[649] A este respecto se manifiesta LÓPEZ, A.: "La investigación…" ob. cit. p. 69.

[650] SIEBER, U.: "Criminalidad Informática: peligro y prevención" en MIR PUIG, S. *Delincuencia Informática*, Ed. PPU, 1ª edición, Barcelona, 1992, pp. 13 y 14, señala que los delitos informáticos no dejan huellas.

[651] La preocupación por este extremo se manifiesta en RUILOBA CASTILLA, J. C.: "La actuación…" ob. cit. p. 62, "una de las medidas actualmente más urgentes es dotar de más efectivos a los grupos

relativamente novedosos, aplicados a las nuevas tecnologías, como pueden ser la vigilancia electrónica sobre teléfonos móviles (u otros sistemas informáticos) o la entrada y registro electrónico[652], se plantean otros problemas relativos al derecho a un proceso de garantías.

B) EN EL ÁMBITO PROCESAL

Además de que perseguir este tipo de delitos puede convertirse en un reto técnico para las fuerzas del orden, la trasnacionalidad también supone problemas en su vertiente jurídica, esto es, el proceso de investigación y de puesta a disposición del sujeto o los sujetos activos desde su localización hacia el Estado que los reclama en relación con el problema de la eficacia de la ley penal en el espacio[653], cuestión que no está exenta de problemas, especialmente cuando los ataques informáticos se producen en Estados con un débil marco jurídico o con otros problemas similares[654]. Problema que por suerte se encuentra resuelto y agilizado en la Unión Europea gracias a los avances legislativos de la última década y que, en menor medida, también encuentra un marco operativo básico entre los Estados firmantes del

---

especializados en la lucha contra la ciberdelincuencia, ya que el número de investigaciones aumenta considerablemente, permaneciendo invariable el número de funcionarios dedicados a su investigación". También referido a la importancia de contar con especialistas formados y medios adecuados, ADÁN DEL RÍO, C.: "La persecución…" ob. cit. pp. 160 y 161. También el actual Ministro de Defensa, ya durante su época como Secretario de Estado de Seguridad en MORENÉS ÁLVAREZ DE EULATE, P.: "Nuevas…" ob. cit. pp. 377 y 378.

[652] ORTIZ PRADILLO, J. C.: "Hacking legal al servicio de la investigación criminal: nuevos instrumentos para la investigación y prueba de la delincuencia informática" en *Revista de Derecho y proceso penal*, nº 26, 2011, pp. 73 y ss. El mismo autor en VVAA: *Delincuencia informática. Tiempos de cautela y amparo*, Ed. Thomson Reuters Aranzadi, 1ª edición, Navarra, 2012. También FLORES PRADA, I.: *Criminalidad*… ob. cit. pp. 361 y ss.

[653] GUTIÉRREZ FRANCÉS, M. L.: "Reflexiones…" ob. cit. p. 80, señala que "su punto realmente diferenciador y unificador lo hallamos justo en su dimensión transnacional, lo que explica esa radical transformación en materia de «eficacia de la ley penal en el espacio». La necesidad de una revisión profunda de este tema, insistimos, no deriva de la presencia de «lo informático» en las modernas manifestaciones de la criminalidad, sino en esa dimensión transnacional (o supranacional) nueva de la delincuencia actual, facilitada, potenciada o propiciada por la revolución de las altas tecnologías de la información y comunicación electrónica".

[654] RUILOBA CASTILLA, J. C.: "La actuación…" ob. cit. p. 55, expresa que "las investigaciones desembocan constantemente en comisiones rogatorias o acuerdos bilaterales o multilaterales entre países que demoran cuantiosamente el tiempo del esclarecimiento de los hechos, perjudicando gravemente el resultado satisfactorio de la investigación. Ello siempre que en el país al que solicitemos la información el hecho esté también tipificado."

Convenio sobre la Ciberdelincuencia de 2001[655]. Sin embargo, incluso en los Estados firmantes, se encuentran regulaciones que dificultan la investigación de determinadas conductas informáticas[656].

Junto con los problemas técnicos y jurídicos relativos a la trasnacionalidad, aparece además un problema jurídico nacional, y es que normalmente los métodos de investigación de las acciones delictivas relativas al uso de ordenadores pueden producir la vulneración de determinados derechos fundamentales, generalmente

[655] Tales instrumentos tratan de armonizar uno de los problemas procesales que surgen a la hora de perseguir y castigar tales acciones, el del lugar de comisión de los hechos y por tanto la competencia de jurisdicción que debe conocerlos. Sobre el particular se puede consultar CORCOY BIDASOLO, M.: "Problemática…" ob. cit. p. 31, "respecto del lugar donde se entiende cometido el delito existen tres construcciones jurídicas que posibilitan la solución de este problema. Son las teorías de la acción, del resultado y de la ubicuidad. Es precisamente esta última la que se ha impuesto, tanto en derecho comparado como en nuestra doctrina y jurisprudencia. De acuerdo con la teoría de la ubicuidad el delito se entiende cometido tanto en el lugar donde se produce el resultado como donde se lleva a efecto la conducta. Ello no excluye la cuestión de la competencia porque, de acuerdo con la teoría de ubicuidad, todos los Estados en los que se ha realizado la conducta y/o producido los resultados tendrían competencia. La solución a esta cuestión de competencia debería solventarse a través del principio de personalidad. Es decir, de entre todos los Estados en principio competentes, sería competente aquel del que sea nacional el autor. En el ámbito de la delincuencia informática puede adquirir una especial relevancia este principio, conforme al cual el Estado de origen del sujeto también tiene competencia para juzgar los hechos cometidos en otro Estado, aunque en él no se haya realizado la conducta ni producido los resultados. Esta solución resulta conflictiva, sin embargo, en los supuestos de coautoría de personas nacionales de diversos Estados y cuando la conducta no es ilícita o tiene una naturaleza diferente en uno y otro. A ello se suman los problemas derivados de la existencia o no de Tratados de extradición, del contenido de esos Tratados y de la reticencia generalizada, por parte de todos los Estados, de entregar a sus nacionales para que sean juzgados en otro Estado". En el mismo sentido, VELASCO SAN MARTÍN, C.: *La jurisdicción y competencia sobre delitos cometidos a través de sistema de cómputo e internet,* Ed. Tirant lo Blanch, 1ª edición, Valencia, 2012, pp. 199 y ss., VELASCO NÚÑEZ, E.: "Cuestiones…" ob. cit. pp. 269 y ss. Con matices en el ámbito de los delitos que no son de resultado se manifiestan SÁNCHEZ GARCÍA DE PAZ, I. y BLANCO CORDERO, I.: "Problemas de derecho penal internacional en la persecución de delitos cometidos a través de internet" en *Actualidad Penal*, nº 7, 2002, pp. 184 y ss. Un ejemplo de conflicto entre la legislación Italiana y Suiza y la aplicación del principio de ubicuidad se desarrolla en FOGGETTI, N.: "Análisis…" ob. cit. pp. 42 y ss.

[656] SÁNCHEZ SISCART, J. M.: "Cibercrimen…" ob. cit. pp. 38 y ss., enumera la situación creada con los Estados Unidos de América, en la que las solicitudes relativas a delitos graves son respondidas por las autoridades norteamericanas bajo cumplimento de ciertos requisitos de información (incluso pueden realizarse peticiones directamente a los prestadores de servicios sin auxilio judicial en determinadas situaciones), en contraste con aquellos casos relativos a delitos menos graves, en los que la colaboración con las autoridades se vuelve difícil y poco flexible. También hace referencia a ello GUTIÉRREZ FRANCÉS, M. L.: "Reflexiones…" ob. cit. p. 76.

reconocidos constitucionalmente[657], lo que llegado el caso puede dar lugar a la nulidad probatoria de las pruebas recabadas que no hayan sido obtenidas con el máximo respecto de los derechos afectados[658]. Ambas realidades en el ámbito procesal de este tipo de delitos suscitan la posibilidad de que no sólo los delitos informáticos en el plano jurídico penal merezcan una revisión, sino también en el ámbito procesal, para amoldar criterios informáticos en el enjuiciamiento criminal de estas acciones[659].

Además cabe señalar que el artículo 264.4 CP habilita la imputación por tales delitos a las personas jurídicas, en la línea seguida por el legislador para los delitos patrimoniales. Sobre este extremo, en realidad, poco cabe añadir a lo ya mencionado, puesto que si bien desde un punto de vista de imputación puede resultar interesante tal posibilidad, desde el punto de vista de la técnica necesaria para la persecución de las acciones delictivas analizadas, normalmente la mayor parte de los problemas van a derivar de la capacidad personal del atacante y su habilidad para no dejar rastro de sus acciones en la red. Que tales acciones se realicen bajo el cobijo de una organización criminal, o incluso con los medios puestos a su disposición por una compañía con fines generalmente lícitos (una compañía de venta de ropa online

[657] SÁNCHEZ SISCART, J. M.: "Cibercrimen…" ob. cit. pp. 37 y 38, "la investigación del cibercrimen aboca principalmente, como métodos principales de investigación u obtención de pruebas, al registro del equipo o sistema informático, o a la interceptación o averiguación de datos de conexiones electrónicas Ambos inciden en planos abarcados por la protección del derecho a la intimidad, inviolabilidad del domicilio, o secreto de las comunicaciones (artículo 18 de la Constitución Española), lo que determina en nuestro ordenamiento interno la necesidad de autorización judicial habilitante, debidamente motivada, que deberá ponderar la necesariedad y proporcionalidad de estas medidas inherentes". En el mismo sentido VELASCO NÚÑEZ, E.: *Delitos*… ob. cit. pp. 73 y ss., y VELASCO NÚÑEZ, E.: "Cuestiones…" ob. cit. pp. 280 y ss. También LÓPEZ ORTEGA, J. J.: "La admisibilidad de los medios de investigación basados en registros informáticos" en *Cuadernos de derecho judicial*, nº 9, 2002, pp. 77 y ss. Ya nos hemos referido a esta cuestión en el capítulo segundo de la investigación al desarrollar la idea de cooperación internacional en el ámbito del Convenio sobre la Ciberdelincuencia de 2001 y la posición a este respecto del TEDH, PÉREZ GIL, J.: "Medidas…" ob. cit. pp. 1815 y ss.

[658] VELASCO NÚÑEZ, E.: *Delitos*… ob. cit. pp. 197 y ss.

[659] PICOTTI, L.: "Internet y Derecho penal: ¿un empujón únicamente tecnológico a la armonización internacional?" en ROMEO CASABONA, C. M. (dir.): *El cibercrimen, nuevos retos jurídico-penales, nuevas respuestas político criminales*, Ed. Comares, Granada, 2006, p. 364, donde determina que no sólo es necesaria una nueva reestructuración de las prácticas informáticas en el ámbito del derecho penal sustantivo, sino que se hace necesaria una nueva regulación procesal penal para una completa vigilancia de estas prácticas delictivas.

contrata a un experto en informática para realizar un ataque sobre la web de la compañía rival) puede, sólo parcialmente, dificultar la persecución, sin embargo, la complejidad de la misma sigue radicando en la capacidad personal del sujeto que realiza el ataque.

Por último, se puede recordar que todo lo señalado anteriormente, además, y por la trascendencia que adquirirá en las próximas páginas, es igualmente aplicable a artículo 197.3 CP, así como a la mayor parte de delitos informáticos.

3. EVALUACIÓN DE LA TRASPOSICIÓN DE LA NORMATIVA INTERNACIONAL DE DAÑOS INFORMÁTICOS

A) TRASPOSICIÓN DE LA NORMATIVA INTERNACIONAL

La actual regulación de los daños informáticos en el Derecho penal español responde, como se ha señalado en repetidas ocasiones, a las orientaciones impuestas en el seno de la Comunidad Internacional. En primer lugar a través del Convenio sobre la Ciberdelincuencia de Budapest de 2001 y en segunda instancia a través de la normativa europea en la materia, que a falta de la próxima aprobación de la Directiva relativa al ataque contra los sistemas de información, se encuentra en la Decisión Marco 2005/222/JAI del Consejo. Aunque la regulación de los daños informáticos no es totalmente novedosa en nuestra normativa, pues ya existía el tipo penal antes de la reforma operada por la LO 5/2010 de 22 de junio, la estructura del actual artículo 264 del Código penal sí lo es, y se debe en parte a las imposiciones internacionales en la materia. No debemos por tanto perder de vista las acciones que en el ámbito internacional se han considerado merecedoras de reproche penal, tanto desde una perspectiva negativa en cuanto a los límites impuestos, como desde un punto de vista positivo, relativo a la libertad que para su tipificación se ha concedido a los Estados.

Los daños informáticos como los entiende hoy nuestra regulación penal, con esta nomenclatura[660], aparecen por primera vez, aunque sin rúbrica, en el informe

[660] En realidad "*Damage to or modifications of computer data or programs*" (Daños o modificaciones de datos o programas informáticos) según ONU: "Manual… ob. cit. pp. 14 y 15.

"Delitos de informática: análisis de la normativa jurídica de la OCDE" en 1986[661] y más tarde en el "Manual de las Naciones Unidas sobre prevención y control de delitos informáticos" de 1994, aunque en ambos casos engloba dos conductas similares que, por el contrario, el Consejo de Europa en 1989 había preferido diferenciar en su listado de delitos informáticos, señalando por un lado los denominados daños contra datos o programas informáticos y por otro lado el sabotaje informático[662]. Por su parte, la Unión Europea no hace una referencia unitaria de los daños informáticos, al incluir estás prácticas junto con otras en su primera Comunicación al respecto de 2001[663].

En cuanto al Derecho internacional impositivo, el Convenio sobre la Ciberdelincuencia de 2001 tampoco establece una categoría concreta de daños informáticos, y tipifica las conductas de daños sobre programas o datos informáticos, y la de obstaculización de sistemas informáticos bajo dos artículos diferenciados[664]. Exactamente en la misma línea quedan recogidas ambas conductas en la normativa de la Unión Europea a través de la Decisión Marco 2005/2228JAI del Consejo que establece ambas conductas con diferentes denominaciones y en artículos diferenciados[665], extremo que además parece mantenerse en la futura Directiva que sustituya dicha Decisión[666].

[661] OCDE: "Computer-related crime…" ob. cit.

[662] Así los clasificaba la Recomendación R(89)9 del Consejo de Europa: Daño a datos o programas informáticos entendidos como borrar, dañar, deteriorar o suprimir datos o programas informáticos sin autorización; y sabotaje informático entendido como la introducción, alteración, borrado o supresión de datos o programas informáticos, u otra interferencia informática con el objeto de obstaculizar el funcionamiento de un ordenador o sistema de telecomunicaciones.

[663] En la COM(2000)890 final, de 26 de enero de 2001. Simplemente engloba estas conductas, junto con otras como la estafa, falsificación, distribución de virus o el espionaje informático bajo la rúbrica de delitos económicos, de acceso no autorizado y de sabotaje.

[664] El artículo 4 denominado interferencia de datos que recoge los daños sobre datos y programas informáticos y el artículo 5 denominado interferencia en el sistema que recoge la obstaculización del funcionamiento de sistemas informáticos.

[665] El artículo 3 tipifica la intromisión ilegal en los sistemas de información y el artículo 4 la intromisión ilegal en los datos.

[666] La propuesta de Directiva relativa a los ataques contra los sistemas de información traslada los artículos 3 y 4 a los nuevos artículos 4 y 5 respectivamente, manteniendo inalterado tanto el título establecido para dichas acciones como su contenido.

Se puede por tanto señalar que, bajo la denominación de daños informáticos genérica que realizan algunos listados, se incluyen en realidad dos acciones diferentes, bien de daños informáticos, bien de sabotaje informático, que nuestro Código penal engloba en su artículo 264, dedicando su primer apartado a los daños sobre datos, programas informáticos o documentos electrónicos (daños), y en el segundo apartado las acciones de obstaculización o interrupción de sistemas informáticos (sabotaje). Respecto a la denominación de las acciones, lo único que se puede extraer de las rúbricas del Código penal es que nos encontramos ante delitos de daños, incardinados bajo los delitos de contra el patrimonio y el orden socioeconómico; en ningún caso el Código pone nombre a dichas acciones, por lo que su nomenclatura general puede generar dudas.

En nuestro estudio nos hemos referido siempre a los daños informáticos como un concepto general en el que se han introducido tanto las acciones de daños informáticos concretos como las acciones de sabotaje informático. El motivo de dicha nomenclatura deriva del hecho de que, siguiendo con el tenor literal tanto del Convenio sobre la Ciberdelincuencia de 2001, como de la Decisión Marco de 2005, así como la regulación derivada de la reforma penal de 2010[667], el sabotaje informático parece más un subtipo penal del daño informático que un tipo penal autónomo. Según la literalidad del artículo 264 -este ejercicio llevaría a los mismos resultados utilizando el Convenio o la Decisión- en el apartado primero se tipifica una acción consistente en dañar datos, programas informáticos o documentos electrónicos, mientras que en la acción típica del apartado segundo lo que se pretende es, con esencialmente las mismas acciones, producir un resultado concreto, esto es, la obstaculización o interrupción de un sistema informático. Por tanto, aunque en la realidad literal, se vuelven a enumerar las acciones, bien podría el legislador haber añadido una clausula remisiva en las acciones de sabotaje informático en la que señalase como causas de la obstaculización o interrupción "las acciones del apartado (o artículo) anterior", en lugar de volver a enumerar dichas acciones.

[667] También de las definiciones de ambas acciones según el listado de la OCDE de 1986 y de la Recomendación del Consejo de Europa de 1989.

Por ello, aunque ambos tipos penales de daños y sabotaje se encuentran autónomamente regulados en la mayoría de las clasificaciones y regulaciones nacionales e internacionales, la realidad es que su interrelación va más allá de la simple conexión lógica que se puede presuponer al hablar de delitos relacionados con los sistemas informáticos y resultan, en definitiva, uno -el de sabotaje informático- un tipo derivado y concreto del otro -el de daño informático-. Sin embargo esto no ha sido siempre así en el caso español. Ya se ha señalado que la actual regulación de los daños informáticos se ha producido a través de dos formas diferentes desde su introducción en nuestro ordenamiento penal en 1995. El antiguo artículo 264.2 CP tipificaba exclusivamente los daños informáticos en sentido estricto, y no hacía referencia al sabotaje informático, aunque como hemos señalado, las acciones de sabotaje informático en ocasiones se han subsumido a través de la jurisprudencia en la acción de daños informáticos[668].

Sentada esta premisa inicial podemos afirmar entonces que, *a priori*[669], el objetivo que persigue la regulación actual de los daños informáticos en España responde de forma estricta -al menos en cuanto al contenido de las acciones penalmente reprochables- a las direcciones internacionales marcadas tanto en el Convenio de 2001 como en la Decisión Marco de 2005 y que la modificación legislativa operada en nuestro ordenamiento por la LO 5/2010 de 22 de junio de reforma del Código penal, ha venido a asemejar las conductas reguladas en el ámbito internacional y europeo con las reflejadas en el Código penal.

[668] Lo que viene a reforzar la idea de que el sabotaje informático es, esencialmente, un subtipo de los daños informáticos. Ya tratamos está cuestión en el capítulo tercero de esta investigación al señalar que la SJP número 2 de Lleida 33/2006 de 7 de febrero, condenaba por un delito del antiguo artículo 264.2 CP un ataque DDoS.

[669] Dicha afirmación debe ser matizada, pues aunque la literalidad de los preceptos en nuestro texto penal es adecuada a la recogida en los textos internacionales, existen otros puntos de controversia que serán analizados en el epígrafe siguiente relativo a la ubicación de los tipos penales, la adecuada protección del bien jurídico y otros aspectos que superan a la mera trasposición literal del precepto.

B) PUNTOS CRÍTICOS DE LA TRASPOSICIÓN. LA DIFUSIÓN DE VIRUS INFORMÁTICOS Y OTRAS ACCIONES SIMILARES

Sin embargo, aunque la literalidad del articulo 264 CP vigente responde adecuadamente al camino marcado por el Derecho internacional, es decir, el legislador ha realizado su labor de trasposición al Derecho interno, al menos textualmente, la normativa internacional en relación a los daños informáticos referidos encuentra algunos puntos críticos en su transposición dignos de mención. No debemos olvidar que España debe introducir en su ordenamiento tanto las disposiciones procedentes del Convenio sobre Ciberdelincuencia de 2001 como de la Decisión Marco de 2005, por lo que desde esa perspectiva debemos revisar las disposiciones de estos dos instrumentos de Derecho internacional.

En primer lugar atendiendo a lo dispuesto en el Convenio de 2001, cabe señalar que existe una tercera acción, vinculada a los daños informáticos, pero sin ser propiamente una acción de dicho ámbito, denominada abuso de dispositivos[670]. En ella se impone a los Estados la necesidad de legislar en materia penal para castigar, al menos, la venta, distribución u otra forma de puesta a disposición de dispositivos (incluidos un programas informáticos), diseñados o adaptados principalmente para la comisión de, además de otros, los delitos de daños informáticos ya analizados[671]. En este sentido, en cuanto a la transposición de la Decisión Marco de la Unión Europea de 2005 no existe conminación respecto a estas acciones, pero es igualmente cierto que la nueva Directiva en trámites de aprobación sí contempla ya la penalización del abuso de dispositivos, de forma similar a la realizada en el Convenio del Consejo de Europa, lo que parece indicar, si no lo era ya, la necesaria reforma de nuestro Código penal en este aspecto.

La introducción de este tipo penal no es baladí, ni puede concluirse que sobrepasa, en todos los casos, el principio de mínima intervención del Derecho penal,

[670] Acciones recogidas en el artículo 6 de Convenio sobre la Ciberdelincuencia de Budapest de 2001.

[671] El artículo 6 recoge las acciones de producción, venta, obtención para su utilización, importación, difusión u otras formas de puesta a disposición, aunque en su artículo 6.3 matiza la obligación de tipificación de los Estados, no exigiendo a los Estados la tipificación de la producción, la obtención para la utilización o la importación de estos dispositivos o programas informáticos.

a pesar de que por su lectura pudiera parecerlo[672], como justificaremos más adelante. La tipificación de esta conducta subsume, tanto por su redacción en el Convenio como por la presumible redacción en la futura Directiva de la Unión Europea, la difusión de virus informáticos en la redes de comunicaciones (Internet). Esta acción, que sí está estrechamente ligada a las acciones de daños informáticos, está actualmente fuera de la regulación penal en España. En efecto, según nuestro ordenamiento penal crear un virus informático, cuyo objetivo principal es afectar al normal funcionamiento de los sistemas informáticos, no está penado -si acaso a través de una suerte de complicidad o cooperación en algunos casos-. Igualmente, tampoco se encuentra penada la distribución de virus informáticos sino en la medida en que esta distribución produzca unos resultados dañinos sobre datos o sistemas informáticos, si bien dicha acción, en función de las posibilidades reales de afectación sobre datos o sistemas informáticos, podría subsumirse dentro de alguna de las anteriores en grado de tentativa, lo que, aun siendo en la práctica procesal penal posible, no parecería la forma idónea, principalmente porque la tentativa en los delitos de daños informáticos se construye de forma compleja como ya fue expuesto en su momento[673], y porque acciones como la mera difusión de un virus informáticos en Internet, que recordamos son capaces de autorreplicarse, complicaría la imputación concreta de daños informáticos al ignorar, en realidad, cual es el resultado o el eventual resultado al desconocer los sistemas informáticos que podrían verse afectados.

Precisamente para evitar esta realidad más que frecuente en la actualidad, el Convenio regula, como un delito de peligro, la difusión de virus informáticos, de tal manera que no sea necesaria la producción de un resultado. La tipificación de esta conducta en nuestro Derecho penal no sólo es recomendable, sino que además es una exigencia de los acuerdos internacionales ratificados por España. En el ámbito de la Unión Europea, si bien no están tipificadas estás conductas, como se ha señalado, es

[672] QUINTERO OLIVARES G.: *Parte*… ob. cit. p. 75.

[673] Recordemos que en el capítulo tercero de la investigación, a la hora de referirnos al grado de ejecución señalábamos la complejidad que se deriva de la inmaterialidad y de la posibilidad de copia exacta del objeto material, lo que planteaba serias dudas en torno al límite entre la tentativa acabada y el delito consumado.

previsible que en poco tiempo sean una realidad, lo que supone una señal más para la necesidad de reformar el actual artículo 264 CP.

4. PRINCIPALES DUDAS QUE SE PLANTEAN EN TORNO AL ACTUAL MODELO DE REGULACIÓN

Además de los conflictos ya analizados que surgen respecto de la dificultad de persecución, y los derivados de una trasposición incompleta, pueden aparecer otras dudas relacionadas directamente con la forma en que nuestro Código penal regula estas conductas, principalmente derivadas de la sintaxis que ha elegido el legislador para tipificar las acciones, así como de su ubicación en el Código como delitos de daños. A lo largo de la investigación se ha dado cuenta de aquellos extremos de la regulación penal que generan problemas de interpretación, sobre los que cabría centrar una futura reforma para evitar una labor interpretativa excesiva de los tribunales de justicia o la aparición de estudios doctrinales contradictorios entre sí. A continuación se exponen sustancialmente estos elementos y las propuestas para una adecuada superación de las dudas que han planteado.

A) COMISIÓN POR MEDIOS FÍSICOS O MEDIOS INFORMÁTICOS

Siguiendo con la distinción que establecimos en el capítulo tercero en cuanto a los modos de realizar las acciones del artículo 264 CP, surgen dudas sobre la idoneidad de la regulación al equiparar a cualquier autor de daños informáticos, no importando los conocimientos que posea.

Esto se deriva del hecho de estar tipificado como un delito común, y no existir una circunstancia agravante específica al respecto. La misma pena -en su marco abstracto- se impondrá al autor del delito de daños informáticos que cometa la acción típica a través de medios informáticos, que al que realiza la acción ejerciendo daños sobre los dispositivos físicos donde se encuentran los datos, programas informáticos o documentos electrónicos. Es más, con la actual regulación, aquel que ejerce la acción de esta segunda forma, cometiendo daños físicos para conseguir el daño informático, sufrirá una penalidad superior, que el que ha realizado el mismo

daño informático a través exclusivamente de un medio informático[674]. La agravación de la pena deriva de la aparición de un concurso medial en el primer caso, en el que el daño físico se realiza como medio para conseguir el daño informático, lo que explica la mayor penalidad de la acción (concurso medial que castiga la acción con la mitad superior de la mayor de las penas previstas en cada tipo penal). Situación que aparecerá siempre en el caso de que el daño físico sea el medio elegido por el autor para la comisión del daño informático.

Sin embargo, como hemos venido señalando en esta investigación, nos parece adecuado apuntar por ahora que, en nuestra opinión, la normativa internacional que ha venido a establecer la necesidad de tipificar estas acciones en nuestro Derecho penal, busca a través de ello proteger un bien jurídico superior al mero patrimonio del sujeto pasivo de estos delitos, y este bien podría designarse como "la seguridad en los sistemas de información". Aunque sobre este planteamiento novedoso nos detendremos más adelante, cabe preguntarse al tenor de los instrumentos internacionales, preocupados por el crecimiento de la ciberdelincuencia y la comisión de atentados contra la integridad tanto de los datos informáticos (programas y documentos electrónicos) como de los sistemas informáticos en su conjunto, si no existe una diferencia de fondo, realmente sustancial, entre la comisión de los delitos de daños informáticos cuando estos se producen a través de daño físico, de aquellos que se producen utilizando medios informáticos. Son estos segundos los que especialmente preocupan a los organismos internacionales, y de alguna manera no explícita, es en estos casos cuando el poder punitivo debe actuar con mayor fuerza[675].

Creemos lógica esta preocupación, pues mientras la producción de daños informáticos a través de medios físicos implica las limitaciones habituales en la

[674] En abstracto, MAZUELOS COELLO, J. F.: "Consideraciones sobre el delito de daños informáticos, en especial sobre la difusión de virus informáticos" en *Derecho Penal y Criminología: Revista del Instituto de Ciencias Penales y Criminológicas*, vol. 28, nº 85, 2007, pp. 29 y 30, afirma que el delito de daños informáticos sólo debe poder ser cometido a través de medios informáticos. Situación que ya ha sido debatida en esta investigación, con una respuesta contraria, al tratar sobre los modos de cometer las acciones según queda redactado el actual artículo 264 CP en el capítulo tercero.

[675] Sobre la mayor trascendencia de los daños cometidos por medios informáticos GONZÁLEZ RUS, J. J.: "Protección…" ob. cit. (sin numerar), que señala que "aunque los daños pueden producirse tanto por procedimientos físicos como propiamente informáticos, son éstos los que despiertan mayor interés."

comisión de los delitos de daños clásicos -presencia física del sujeto atacante o del arma con el que pretende realizar el daño físico, ataque a un número determinado (mayor o menor) de objetos, etc.- es muy diferente el caso de los daños informáticos cometidos a través de medios informáticos, en el que una sola persona, con un ordenador y conexión a la red, puede realizar alguno de los tipos de daños informáticos en un número indeterminado de sistemas informáticos (eventualmente, contra absolutamente todos los sistemas conectados a la red) sin necesidad de desplazamiento físico o limitación de posibles víctimas. Acciones cuya gravedad y repercusión son sustancialmente diferentes y que quedan divididas, además de por el medio, por el sujeto que las comete, siendo el de las segundas un peligro potencialmente mayor para la sociedad.

En resumen, en España, con la actual regulación, pueden cometerse los daños informáticos a través de daños físicos o de medios informáticos. A los primeros, generalmente, se les castiga con mayor penalidad por la aplicación de las reglas de determinación de la pena contenidas en el Libro I de nuestro Código penal -concurso medial del artículo 77 CP-. Sin embargo, de los instrumentos internacionales relativos a la lucha contra la criminalidad informática, se puede fácilmente extraer que la preocupación de las instituciones reside fundamentalmente en los daños informáticos cometidos por medios informáticos, que precisamente con la actual regulación presentan a priori, menor penalidad que los primeros. En todo caso, quizá la vía de resolver este tipo de conflictos, al menos siguiendo la sistemática del Código penal español, pasaría por crear una mención expresa a ello, o bien en los delitos de desórdenes públicos, o incluso en los de terrorismo para determinados casos concretos (al margen del ya existente 577 CP)[676].

B) DOBLE GRAVEDAD EXIGIDA EN EL TIPO

Otro de los extremos que genera incertidumbre en la actual regulación es la exigencia de doble gravedad que se establece en los dos tipos penales del artículo

[676] Cuando estos delitos tengan como finalidad influir en aquellos que toman decisiones políticas a través del atentado contra las libertades de un tercero, el ciudadano, así, ZUGALDÍA ESPINAR, J. M.: "Terrorismo y globalización" en LÓPEZ CALERA, N. M. (coord.): *La palabra contra el terrorismo*, Ed. Universidad de Granada, 1ª edición, Granada, 2004, p. 71.

264 CP. Para que la acción se considere típica el daño debe perpetrarse "de manera grave" y demás producir un resultado grave. Sobre las dudas que se pueden suscitar en torno a la gravedad del resultado nos detendremos más adelante, ocupándonos ahora de la primera exigencia de gravedad[677]. La previsión de la gravedad en el método de comisión del delito no encuentra, desde luego, su origen en la tipificación internacional de las conductas, en las cuales la única gravedad mencionada es la del resultado, y la doctrina en España tampoco ha sabido dar una respuesta inequívoca al respecto sobre si se trata de una repetición efectuada por el legislador (supuesto difícilmente verificable) o si se trata de un límite al modo de comisión (lo que entraría en conflicto con el elemento "por cualquier medio") .

Ante la falta de información al respecto y las dificultades que este elemento suscita, en esta investigación se ha propuesto ya la posibilidad de entender esta gravedad como la idoneidad de la conducta empleada para la consecución del fin perseguido (los daños informáticos). Sin embargo, esta extensión semántica del significado de las propias palabras de los preceptos penales no parece tampoco recomendable, siendo necesario, llegado el momento, proceder o bien a su sustitución por otra fórmula como la propuesta, o bien su supresión como elemento del tipo, pareciendo esta segunda opción la más recomendable por eliminar definitivamente un elemento que se ha confeccionado más bien como un factor de incertidumbre del tipo penal.

C) GRAVEDAD DEL RESULTADO: EL VALOR ECONÓMICO DEL DAÑO INFORMÁTICO

Para entender la gravedad en el resultado que se exige en los daños informáticos en primer lugar cabría referirnos a la ubicación que encuentran las acciones en nuestro Código penal. Si bien la regulación internacional de la que deriva la actual normativa no señala un ámbito concreto en el que incardinar dichas conductas, en la realidad del ordenamiento jurídico penal español es importante

[677] La discusión en torno a esta cuestión se trató en el capítulo tercero, en el apartado dedicado a la doble exigencia de gravedad del tipo penal del artículo 264.1 CP. Baste señalar simbólicamente la expresión en QUERALT JIMÉNEZ, J. J.: *Derecho*… ob. cit. p. 641, donde se afirma que "estos dos requisitos típicos presentan no pocas complejidades […] Las locuciones del legislador generan perplejidad en el intérprete".

conocer dónde se encuentran incardinadas determinadas acciones típicas y porqué, pues la organización del propio Código penal responde a la protección de diversos bienes jurídicos. Así encontramos que, siguiendo con la ubicación realizada por el Código penal de 1995, los daños informáticos se encuentran en el Capítulo IX (delitos de daños), del Título XIII (delitos contra al patrimonio y el orden socioeconómico) del Libro II (de los delitos y sus penas). En las próximas líneas vamos a recordar la trascendencia que esto tiene en la actual regulación y la interpretación que debemos hacer cuando los tipos se refieren a la producción de un resultado grave, así como los problemas que pueden surgir.

Por su ubicación sistemática en el Código penal, los daños informáticos son considerados por el legislador delitos de daños patrimoniales[678]. Superada la discusión sobre su carácter autónomo o vinculado a los daños clásicos del artículo 263 CP con la entrada en vigor de la LO 5/2010 de 22 de junio, que los configuran claramente como un tipo autónomo de daños, debemos señalar que dicha modificación del texto penal los mantiene dentro del Capítulo relativo a los daños, y por tanto, existen ciertos puntos comunes -o así sería lógico entenderlo- que deben interpretarse igualmente, hablemos de daños clásicos del artículo 263 CP o de daños informáticos del artículo 264 CP. El principal elemento en común es el que hace referencia a la producción del resultado en este tipo de delitos. Ya hemos señalado en la investigación que existe una diferencia básica entre el resultado en los daños del artículo 263 CP, que requieren que el valor patrimonial de lo dañado sea superior a 400 euros, y el resultado en el daño informático, en el que el valor económico de lo dañado debe ser grave, sin la imposición de un límite cuantitativo por parte del legislador. Pero en lo que ahora queremos detener nuestro análisis es en la forma de cuantificación de ese valor patrimonial de los efectos destruidos, pues la gravedad del resultado, en todo caso, al incluirse los delitos informáticos entre los delitos de daños, debe ser referida al valor económico de lo dañado, lo que supone un límite a

[678] Por todos, como ya se ha señalado en el capítulo tercero de esta investigación, DE LA MATA BARRANCO, N. J. y HERNÁNDEZ DÍAZ, L.: "El delito…" ob. cit. p. 332, "al margen de lo que sea que tutele […] su ubicación sistemática obliga a entenderlo patrimonialmente". En el mismo sentido FARALDO CABANA, P.: *Las nuevas*… ob. cit. 143, establece que hablamos de bienes "de contenido económico", aunque abre la puerta a la interpretación dispar de los elementos del tipo de daños informáticos (especialmente la gravedad del resultado) de la tradicional realizada para los daños clásicos.

la aparición típica, si se entiende, como debería, de forma análoga a los daños clásicos.

Ya se ha señalado en esta investigación que, en la concepción clásica del delito de daños, el coste de la reparación de todo daño debe contabilizarse exclusivamente como responsabilidad civil, de la misma forma que el lucro cesante por la imposibilidad de utilizar lo dañado[679]. Igualmente hemos apuntado, y conviene ahora recordarlo, que en los daños informáticos, siempre y cuando nos encontremos ante un propietario diligente de los datos, programas informáticos o documentos electrónicos, rara vez se produce el daño entendido de la manera clásica (lesión de la propiedad mediante el ataque a la integridad material de la cosa). La mera existencia de copias de seguridad de los datos o los sistemas informáticos en su conjunto elimina la posibilidad de que se produzca un daño patrimonial en el sentido clásico del mismo (se produciría en todo caso la tentativa, pero rara vez la consumación del tipo) y puesto que el coste de la reparación de esos datos o sistemas informáticos, y el lucro cesante provocado por el *iter* en los que no han estado disponibles tampoco puede ser considerado para contabilizar el valor económico de lo dañado, nos encontramos con que, en la mayor parte de los casos de ataques informáticos con la finalidad de realizar estos daños, no se produce realmente un daño en el sentido patrimonial clásico de los daños, lo que plantea el indudable problema sobre si esa cuantificación económica de los daños debe realizarse bajo los mismos límites en el caso de los daños clásicos y de los daños informáticos[680].

En efecto, la relevancia del daño informático, atendiendo a la realidad a la que pertenece, no radica tanto en la destrucción definitiva o deterioro sustancial de un objeto y la merma de su utilidad funcional derivada del daño físico sobre el

[679] NÚÑEZ FERNÁNDEZ, J.: "Otras consecuencias…" ob. cit. pp. 950 y ss. Ver *supra:* capítulo tercero, epígrafe dedicado a la doble gravedad exigida por el tipo del 264.1 CP.

[680] MORALES GARCÍA, O.: "Apuntes…" p. 30, ya aventura que si para calcular el daño en el ámbito penal se utiliza el valor que los datos, programas o documentos electrónicos podrían haber tenido o producido "a través de una interpretación funcional, se introduce en el núcleo del injusto un valor propio de la responsabilidad civil derivada del delito", por lo que se plantea si entonces sobre los daños informáticos del artículo 264 CP cabe la doctrina clásica de daños, y el tipo sólo supone una aclaración legislativa para el caso de objetos inmateriales, o si realmente nos encontramos ante conductas típicas que merecen una doctrina autónoma que reconozca sus particularidades.

mismo (concepción clásica de los daños), como en el compromiso de la integridad de cierta información en sentido informático, es decir tanto datos informáticos como programas informáticos que mantienen operativo un sistema de información, y documentos electrónicos que se almacenan en soportes informáticos. Por lo tanto, la interpretación más correcta sobre lo que debe entenderse como valor económico del objeto dañado debe vincularse en estos casos a valor económico de la integridad de esos datos o sistemas informáticos. Es decir, a la afectación de su utilidad desde un punto de vista de operatividad de los datos y sistemas, sin necesidad de que éste sea consecuencia del daño físico[681]. Por tanto, el daño informático se producirá con el menoscabo funcional exclusivamente.

Pero tal afirmación nos conduce a otro problema, ya que para poder cuantificar económicamente el daño informático patrimonialmente hablando, a diferencia de la interpretación de los daños clásicos, sí debe ser considerado como valor económico penalmente cuantificable el coste de restablecimiento de la operatividad del sistema o los datos, pues de lo contrario quedarían impunes una cantidad excesiva de conductas. Además el marco penal abstracto tipificado es suficientemente amplio para dar cabida tanto a daños informáticos cuantificados por la destrucción definitiva de los datos informáticos como el daño recuperable sobre la integridad de los sistemas informáticos, siempre desde la perspectiva de la consumación.

El problema reside en que realizar una distinta valoración de lo que debe entenderse por valor económico de lo dañado si nos encontramos ante daños clásicos o daños informáticos corresponde, en la actualidad, a los tribunales de justicia, y aunque, para una mejor aplicación práctica del Derecho, parece que va a ser necesario que la jurisprudencia se pronuncie en el sentido de crear diferencias en función de unos y otros -como la doctrina ha venido sugiriendo-. No obstante, ante la elección del legislador de ubicar los daños informáticos en el ámbito patrimonial relativo a los delitos de daños, podemos concluir que no sería, sistemáticamente, lo más adecuado, pudiendo ser una posibilidad mejor extraer los delitos de daños

[681] ANDRÉS DOMÍNGUEZ, A. C.: *El Delito…* ob. cit. pp. 149 y 150, refiriéndose a los daños clásicos señala que "se requiere tanto un daño físico […] como un daño funcional".

informáticos del capítulo del Código penal dedicado a los daños, e incluso, de los delitos contra el patrimonio.

D) ENUMERACIÓN DE ACCIONES: ¿LITERALIDAD O EXCESO?

Se han planteado dudas a lo largo del análisis jurídico penal de los delitos de daños informáticos del artículo 264 CP en cuanto a la idoneidad de reunir en los tipos penales de daños informáticos una colección casi indiscriminada de acciones, toda equiparadas, y en ocasiones repetitivas, que son introducidas por el legislador como acciones típicas. Se puede defender que no es cuestión achacable en toda su extensión al legislador nacional, que se ha limitado a repetir la enumeración exacta realizada en la Decisión Marco de 2005. Y, aunque en favor de dicha enumeración en nuestro Código penal debemos señalar que es la forma más exacta de transponer la normativa europea, no debemos por ello obviar algunas dudas que surgen sobre la misma.

Las acciones del artículo 264.1 CP, que luego conforman el núcleo de los modos de cometer las acciones del artículo 264.2 CP, son las que suscitan más interrogantes. Borrar, dañar, deteriorar, alterar, suprimir, o hacer inaccesibles datos, programas informáticos o documentos electrónicos son las seis acciones típicas del artículo 264.1 CP a las que dedicamos un extenso análisis en esta investigación, en el que ya señalamos que todas ellas podrían ser reconducidas a un listado más simple: suprimir, hacer inaccesibles o alterar datos, programas informáticos o documentos electrónicos. Hacer inaccesibles datos, programas informáticos o documentos electrónicos (conducta dentro de la cual, entre otras, se subsume la acción de borrar como medio para conseguir la inaccesibilidad) supone una acción menos grave que suprimir datos, programas informáticos o documentos electrónicos, ya que esta segunda conducta típica implica la completa desaparición de éstos. Por su parte la acción de alterar puede suponer una conducta más o menos grave en función del alcance de la modificación producida, desde un cambio tan sustancial en la integridad de los datos, programas informáticos o documentos electrónico que el resultado sea prácticamente equiparable a la desaparición definitiva al haberse convertido en otros, hasta una acción atípica cuando la alteración sea mínima o,

siendo considerable, no afecte a la utilidad de los datos, programas informáticos o documentos electrónicos originales

Quedarían excluidas de este listado las conductas de dañar y deteriorar, junto a la ya mencionada borrar, por cuanto si la primera acción de dañar no aporta ningún significado concreto, sino que sería la forma más general de señalar la acción típica (como se hace, de hecho, en los daños clásicos del artículo 263 CP); por su parte la acción de deteriorar, en el ámbito informático, quedaría subsumida dentro de la acción de alterar: se configuraría como una alteración que hace perder funcionalidad a los datos, programas informáticos o documentos electrónicos. Por último la acción de borrar (no confundir con la de suprimir), es realmente un método habitual de hacer inaccesibles datos, programas informáticos o documentos electrónicos que realmente no han sido destruidos.

Sentadas estas reflexiones cabe, al menos, hacer una última, y es que, si el legislador internacional -ya que parece que el nacional se ha limitado a trascribir el catálogo- ha decidido hacer esta enumeración de conductas debe de entender que deben ser diferentes, y tales diferencias han de ser ser manifestadas por el juzgador a la hora de determinar los marcos penales concretos en la imposición de penas, así como por la doctrina cuando sean estudiadas. Aceptando esta idea como perfectamente válida, se vuelve a la problemática de determinar qué acciones en principio tienen un mayor desvalor, si bien el legislador, atendiendo a la redacción realizada, las ha asimilado[682].

E) EL BIEN JURÍDICO INMEDIATAMENTE PROTEGIDO.

Quizá este sea el origen de todos los conflictos analizados derivados de la tipificación de los delitos informáticos en nuestro Código penal. En la actualidad no se considera que exista un bien jurídico de entidad suficiente relacionado con los sistemas informáticos que merezca un tratamiento autónomo y una protección penal específica.

[682] MORALES GARCÍA O.: Comentario…" ob. cit. 160, entiende que sobre las diferentes acciones, a la hora de fijar la determinación de la pena, si el legislador hace diferencias, diferentes tienen que ser las consecuencias de unas u otras, aunque nada se diga en el texto del artículo.

El legislador español, siguiendo la preocupación de la Comunidad Internacional, así como de la Unión Europea, ha manifestado su lógica adhesión a la misma tipificando las acciones que suponen un atentado contra la seguridad de los sistemas informáticos, dando cabida a la mayor parte de las exigencias internacionales en nuestro Código penal[683]. Sin embargo, en la actualidad ello no ha supuesto la verdadera consagración de este valor como un bien superior digno de protección penal de primera línea. Así, los delitos de daños informáticos -junto con otros delitos informáticos en sentido amplio- por su ubicación en el Código, protegen principalmente diversos bienes jurídicos, sin renunciar, obviamente, a la idea de seguridad en los sistemas informáticos, lo que, como hemos visto, plantea problemas al quedar limitados por los parámetros comunes de interpretación de todos los delitos con los que se encuentran agrupados.

En consonancia con la preocupación en el ámbito internacional que suscitan estos mismos delitos, parece haberse iniciado un camino en el que, por sí mismos, este tipo de delitos pasen a proteger un bien jurídico de primer orden, pudiendo tutelar, además, otros bienes jurídicos que se manifiesten con menor intensidad (intimidad, patrimonio, etc.), situación que sería inversa a la actual, en la que el bien jurídico protegido principal es aquel relativo al lugar donde se encuentran ubicados en el Código, y en menor medida, son tipos protectores de un bien jurídico indeterminado pero vinculado a la informática. Por todo ello, se hace imprescindible un análisis del punto de vista que sobre este asunto se tiene en la actualidad, así como la proposición de un nuevo modelo que, en nuestra opinión, resolvería algunos de los problemas apuntados y que mostraría de forma más acertada las preocupaciones en el ámbito público internacional, pero fundamentalmente reflejaría de mejor manera la realidad social actual. A este asunto dedicaremos las siguientes páginas de la investigación.

[683] No sólo con la reforma de los daños informáticos, también ha adaptado su normativa penal para sancionar el acceso ilícito, así como ha realizado las modificaciones necesarias en materia de pornografía infantil y protección del menor ante la delincuencia informática. Igualmente ha puesto en funcionamiento medidas de cooperación e investigación de estos delitos que no afectan directamente a la legislación penal.

5. LA MODIFICACIÓN DEL ACTUAL PUNTO DE VISTA

A) LA POSIBLE INTRODUCCIÓN DE UN TÍTULO O CAPITULO EN NUESTRO CÓDIGO PENAL DEDICADO A LA INFORMÁTICA

Tal como ha sido redactado el Convenio sobre la Ciberdelincuencia de 2001 y, en menor medida, como están descritas las acciones merecedoras de reproche penal en la Decisión Marco de 2005[684], puede extraerse la idea de que los delitos informáticos en sentido amplio, tanto si son delitos cometidos a través de la informática como si son delitos cometidos contra sistemas informáticos, responden a una clasificación relativamente cerrada. Tales conductas ya no se pueden considerar nuevas, pues al menos en el ámbito práctico y el ámbito extra penal vienen reflejándose de forma constante desde finales de la década de 1980, siempre agrupadas de una forma muy similar.

En el ámbito penal, consecuencia de ello, se abre el debate sobre la naturaleza de las acciones penales a través de las que se tipifican estos abusos de los sistemas de información, sobre su objeto de protección general y sobre la necesidad, o no, de regular de alguna forma específica aquellos delitos en los que participan con mayor o menor intensidad los sistemas informáticos.

Ya se señaló al comienzo de esta investigación que por delitos informáticos, en sentido amplio, se pueden llegar a entender casi cualquier delito clásico en el que, por el medio de comisión, se ha usado un sistema informático[685], lo que en la práctica se traduce en una complicación extrema de regular los delitos informáticos de forma unitaria en nuestra legislación penal. En cambio, como ya hemos indicado, desde las instituciones internacionales sí se ha introducido un grupo cerrado de tres tipos de acciones que son en las que, en un sentido menos generalista, se pueden subsumir los delitos informáticos en sentido amplio. Estas conductas serían las que engloban delitos en los que los sistemas informáticos son la herramienta fundamental para la

[684] Estructura que se asimilará a la del Convenio cuando finalmente se apruebe el proyecto de Directiva en la materia.

[685] Delitos de injurias o calumnias, o en un caso extremo un delito contra la inviolabilidad de las Cortes (ataque a los sistemas informáticos del Congreso que impiden que se vote alguna medida, por ejemplo).

comisión del delito (estafa y falsificación informática), delitos en los que el sistema informático es el objeto del delito (acceso ilícito y daños informáticos), y delitos relacionados con el contenido, en los que los sistemas informáticos facilitan de forma sustancial la comisión de los mismos (propiedad intelectual y pornografía infantil).

Tal listado respeta sustancialmente las diversas clasificaciones de los estamentos internacionales y al respecto cabe preguntarse si sobre la misma sería posible extraer algunas conclusiones comunes en los delitos que pueda justificar la idea de aglutinarlos en nuestro Código penal dentro de un Título o Capítulo (dentro del Título XXIII del Libro II, pero más vinculado al orden socioeconómico que al delito patrimonial en concreto[686]) que se pudiese denominar "de los delitos informáticos"[687].

a.1. Teoría del bien jurídico protegido en relación con los delitos informáticos

La mayor parte de la doctrina española[688] ha venido a consagrar la idea de exclusiva protección de bienes jurídicos como barrera al poder punitivo del Estado[689], y es en base a la misma conforme a la que se han ordenado, en términos generales, los delitos en el Libro II del Código penal. La teoría clásica de protección de bienes jurídicos como legitimación para la actuación del Estado en materia punitiva[690] ha supuesto la base sobre la que se ha construido nuestro sistema penal vigente. Doctrina que exige, para la justificación de los tipos penales, que las conductas en ellos descritas provoquen -o puedan hacerlo- la lesión de un bien

[686] En los países de nuestro entorno, este es el modelo seguido por el Código penal francés.

[687] URBANO CASTRILLO, E.: "Los delitos…" ob. cit. p. 29, defiende que debería existir un Título diferenciado que distribuya en diferentes capítulos, en los que primaría un bien jurídico protegido único, y unas disposiciones comunes finales a todos los tipos penales. Incluso negando este cambio radical, al menos debería completarse un capítulo de delitos informáticos con aquellos propiamente informáticos y una agravante genérica en los demás, cuando para la comisión del tipo se aprovechasen de la facilidad que otorga el medio informático.

[688] GARCÍA-PABLOS DE MOLINA, A.: *Introducción…* ob. cit. pp. 173 y ss. o QUINTERO OLIVARES G.: *Parte*… ob. cit. pp. 67 y ss.

[689] BACIGALUPO ZAPATER, E.: *Derecho penal. Parte general*, Ed. Hammurabi, 2ª edición, 1999, pp. 43 y 44, señala que "el Derecho penal moderno (a partir de Binding) se ha desarrollado desde la idea de protección de bienes jurídicos. De acuerdo con ella, el legislador amenaza con pena las acciones que vulneran (o ponen en peligro) determinados intereses de una sociedad determinada".

[690] ROXIN, C.: *Derecho…* ob. cit. p. 51.

jurídico[691]. Queda así excluido del poder punitivo del Estado la regulación de meras inmoralidades[692], o como se ha señalado más recientemente, de intereses sociales mayoritarios[693], que no siempre deben ser identificados con un bien jurídico existente. De todo ello se deduce que, si bien se ha manifestado en varias ocasiones la idea de que la seguridad en el campo de la informática y las telecomunicaciones es un campo relevante con un interés social innegable, este hecho no es de entidad suficiente para elevar dicho concepto al nivel de bien jurídico, para lo cual serán necesarios otros requisitos.

Sin embargo, a pesar del conocimiento de lo que un bien jurídico no es, lo cierto es que tampoco existe una definición pacífica en la doctrina que limite el alcance del propio concepto de bien jurídico[694]. La doctrina ha venido a señalar que el punto de partida para la conceptualización de un bien jurídico debe tener origen en la Constitución[695], sin embargo, reconocer la vinculación de la Constitución y el bien jurídico protegido puede ser, en ocasiones, abstracto y complicado[696]. Este hecho le

[691] GARCÍA-PABLOS DE MOLINA, A.: *Introducción…* ob. cit. p. 174, "no se trata de prohibir por prohibir, de castigar por castigar, sino de hacer posible la convivencia y la paz social".

[692] ROXIN, C.: *Derecho…* ob. cit. pp. 52 y 53. En España, MIR PUIG, S.: "Bien Jurídico y Bien Jurídico-Penal como Límites del *Ius Puniendi*" *en Estudios penales y criminológicos*, nº 14, 1991, pp. 205 y ss.

[693] Señalado por GIMBERNAT ORDEIG, E., en la presentación de HEFENDEHL, R.: *La teoría del bien jurídico ¿Fundamento de legitimación del Derecho penal o juego de abalorios dogmáticos?*, Ed. Marcial Pons, 1ª edición, Madrid, 2007, pp. 12 y ss. En MUÑOZ CONDE, F. y GARCÍA ARÁN, M.: *Derecho…* ob. cit. p. 60, se denomina la "perversión del concepto de bien jurídico".

[694] ROXIN, C.: *Derecho…* ob. cit. p. 54. En España, GARCÍA-PABLOS DE MOLINA, A.: *Introducción…* ob. cit. p. 175 o MIR PUIG, S.: *Introducción a las bases del derecho penal: concepto y método*, Ed. Catapulta, 2ª edición, Buenos Aires, 2003 pp. 128 y ss.

[695] ROXIN, C.: *Derecho…* ob. cit. p. 55, "el punto de partida correcto consiste en reconocer que la única restricción previamente dada para el legislador se encuentra en los principios de la Constitución", en el mismo sentido en España, SILVA SÁNCHEZ, J.M.: *La expansión del derecho penal: Aspectos de la política criminal en las sociedades postindustriales*, Ed. Civitas, 2ª edición, Madrid, 2001, pp. 92 y ss. Sin embargo, hay manifestaciones en contra de la idoneidad de esta vinculación, WOHLERS, W.: "Las jornadas desde la perspectiva de un escéptico del bien jurídico" en HEFENDEHL, R.: *La teoría del bien jurídico ¿Fundamento de legitimación del Derecho penal o juego de abalorios dogmáticos?*, Ed. Marcial Pons, 1ª edición, Madrid, 2007, pp. 404 y ss.

[696] Es destacable la compleja construcción doctrinal realizada por GIMBERNAT ORDEIG, E., en la presentación de HEFENDEHL, R.: *La teoría…* ob. cit. p. 17 y 18, para encajar los delitos relativos a la tortura animal, dentro de los valores constitucionales establecidos, en orden a establecer así el bien jurídico que protegen tales tipos penales en nuestro ordenamiento.

ha costado críticas reseñables a dicha teoría[697], pero debemos reconocer que al tiempo la configura de forma que los bienes jurídicos pueden ser revisados y su catálogo ampliado. Esta característica se antoja fundamental si queremos verificar la existencia de un bien jurídico digno de protección penal relacionado con los sistemas de información, pues la concepción actual del bien jurídico abarca tanto estados previos a la concreción del Derecho, como deberes de cumplimiento creados por éste, siendo el caso de la informática el segundo[698]. Pero tanto la mutabilidad del concepto como la sujeción (que no limitación) a los valores constitucionales no debe llevarnos a la conclusión de que no existen límites al concepto de bien jurídico. En general, el bien jurídico penal, es aquel presupuesto necesario para el desarrollo personal y realización de los individuos en la sociedad entre los que encontramos, principalmente la vida o la salud como manifestaciones de lo primero, y la libertad o la intimidad de lo segundo[699]. Estos bienes, además, podrán ser individuales o colectivos[700], siendo estos segundos especialmente relevantes en el ámbito que nos ocupa, pues están vinculados al orden social o comunitario del individuo. Ahora bien, entender que la seguridad de los sistemas de información responde adecuadamente a la teoría del bien jurídico será, en una parte fundamental, una "cuestión valorativa"[701]. Hecha esta apreciación, cabe destacarse que para que podamos hablar de bien jurídico protegido, al menos, debemos encontrarnos ante valores vinculados al reconocimiento constitucional. Además, debe verificarse la existencia de un interés social de protección, entendido en el sentido de cuál será la afectación para el individuo en caso de ser vulnerado y, vinculado con lo anterior, es

[697] JAKOBS, G.: *Derecho penal. Parte general. Fundamentos y teoría de la imputación*, Ed. Marcial Pons, 2ª edición (corregida), Madrid, 1997, pp. 47 y 48.

[698] Las normas penales que regulan la seguridad en los sistemas de información no podían responder a la protección de bienes constitucionalmente recogidos pues en muchos casos son muy posteriores a estos textos constitucionales, sin embargo, ello no obsta para que, una vez producida la aparición de la informática, las normas que la protegen no puedan basar su existencia en nuevos bienes jurídicos sobrevenidos, tan dignos de protección como los originales. ROXIN, C.: *Derecho…* ob. cit. pp. 54 y ss., ejemplifica esta situación con la protección de bienes jurídicos que suponen ciertos delitos tributarios o la provocación de ruidos.

[699] MUÑOZ CONDE, F. y GARCÍA ARÁN, M.: *Derecho…* ob. cit. p. 59.

[700] GARCÍA-PABLOS DE MOLINA, A.: *Introducción…* ob. cit. p. 174, aunque sobre la idoneidad de la teoría del bien jurídico para proteger bienes colectivos veremos en las próximas páginas que existen voces discrepantes.

[701] MIR PUIG, S.: "Bien Jurídico…" ob. cit. pp. 205 y ss., "la apreciación de cuándo un interés es fundamental para la vida social y cuándo no lo es […] se trata de una cuestión valorativa."

necesario graduar el riesgo de afectación del bien jurídico, y por tanto la necesidad de estipular su protección en las normas penales del Estado.

En nuestra búsqueda de un bien jurídico relativo a la seguridad en los sistemas de información debemos realizar igualmente la asociación de los presupuestos anteriores a la realidad de los sistemas informáticos en la actualidad. La vinculación de la seguridad en los sistemas de información y la Constitución aparece en primer lugar su artículo 1 al señalar como uno de los valores fundamentales la libertad y la justicia. Todavía en el Título preliminar se establece que los poderes públicos deberán remover "los obstáculos que impidan o dificulten su plenitud" (artículo 9.2 CE). Ya en el Título primero, el artículo 10 CE consagra el libre desarrollo de la personalidad. Si bien el desarrollo de la libre personalidad es un concepto sumamente general, no escapa a la lógica entender que cuando los sistemas informáticos han pasado a formar parte de la realidad cotidiana de la vida de los ciudadanos, un ataque contra estos sistemas afectará, en función de la intensidad del mismo, al desarrollo de la personalidad[702]. En todo caso parece correcto afirmar que la libertad reconocida en la Constitución va más allá de la mera libertad de circulación o establecimiento, y se configura como una verdadera facultad de autodeterminación personal, en todos los ámbitos propios de la vida de la persona[703]. Siguiendo esta línea de razonamiento debemos buscar la conexión entre la libertad constitucionalmente establecida con la utilización de sistemas informáticos, y verificar si el uso de éstos es una manifestación de la libertad constitucionalmente reconocida, de tal modo que el nexo constitucional requerido para la apreciación del bien jurídico quede establecido. Según nuestra posición, la libertad para utilizar los medios informáticos sin más límite que el derecho de los demás debe, efectivamente, entenderse subsumido en el concepto constitucional tanto del artículo 1.1 como el 9.2 de la Constitución, pues la utilización de estos medios informáticos no es sino una manifestación moderna de la libertad clásica. No se debe confundir esta libertad general, en todo caso, con los ámbitos de la libertad y seguridad establecidos en el

[702] Piénsese en un ataque general contra los sistemas informáticos que gestionan las redes de comunicaciones e Internet que inutilice todos los sistemas de telefonía y de comunicación electrónica en general. Por no hablar de ataques contra el sistema de regulación del tráfico de una ciudad o los sistemas informáticos de plantas de suministro de electricidad.

[703] DE ESTEBAN ALONSO, J. y GONZÁLEZ-TREVIJANO SÁNCHEZ, P.: *Tratado*… ob. cit. p. 76.

artículo 17 de la Constitución, referidos específicamente al derecho de no ser privado de libertad en su manifestación física[704].

También desde un ámbito constitucional de la seguridad en relación con los sistemas informáticos el Estado garantiza el secreto de las comunicaciones (artículo 18.3 CE), lo que desde la óptica que ahora interesa parece ser imposible si no se garantiza la seguridad de las redes de comunicaciones y los sistemas informáticos que en ellas participan. La seguridad -como ocurre con la libertad- viene reflejada en la Constitución desde diversos prismas: seguridad jurídica (artículo 9.2), seguridad personal (artículo 17.1), seguridad social (artículo 41), seguridad ciudadana (artículo 104.1) y seguridad pública (artículo 149.1.29), siendo estas dos últimas las que a nuestro estudio interesan, pues se vinculan estrechamente con la posibilidad de ejercer el derecho a la libertad informática ya señalado y que el Tribunal Constitucional ha interpretado señalando que "la seguridad pública, entendido como actividad dirigida a la protección de personas y bienes y al mantenimiento de la tranquilidad y el orden ciudadano, según pusimos de relieve en las SSTC 33/1982, 117/1984, 123/1984 y 59/1985, engloba, como se deduce de estos pronunciamientos, un conjunto plural y diversificado de actuaciones, distintas por su naturaleza y contenido, aunque orientadas a una misma finalidad tuitiva del bien jurídico así definido"[705]. Por tanto, seguimos pudiendo apreciar la posibilidad de vincular la libertad y la seguridad en los sistemas de información, con el mandato constitucional dado. La libertad es un Derecho general que requiere del establecimiento de un marco de seguridad para su protección[706]. Éste ámbito de la seguridad ha encontrado diverso desarrollo legislativo, principalmente en la LO 2/1986, de 13 de marzo, de Fuerzas y Cuerpos de Seguridad del Estado[707], que establece, en lo que ahora interesa, la organización básica del Cuerpo Nacional de Policía y de la Guardia Civil.

[704] SSTC 71/1994, de 3 de marzo, 86/1996, de 21 de mayo y 120/1999, de 27 de junio.

[705] STC 104/1989, de 8 de junio, FJ. 3.

[706] DE ESTEBAN ALONSO, J. y GONZÁLEZ-TREVIJANO SÁNCHEZ, P.: *Tratado*… ob. cit. p. 79, "este derecho [la seguridad] hay que entenderlo como la garantía jurídica del individuo frente al poder, para evitar no sólo la privación de su libertad, sino también cualquier forma arbitraria de represión".

[707] Manifestación de esta máxima constitucional debe entenderse también la LO 1/1992, de 21 de febrero, sobre Protección de la Seguridad Ciudadana, si bien en la misma no se hace referencia a los sistemas informáticos, por lo que la excluimos de nuestro estudio.

En el caso del Cuerpo Nacional de Policía establece en sus artículos 29 a 36 la estructura básica de la Policía judicial, donde se señala que corresponde al Ministerio del Interior "organizar Unidades de Policía Judicial", atendiendo a criterios "de especialización delictual" (artículo 30.1). Pues bien, con el fin de seguir tal mandato, en la actualidad la estructura orgánica del Cuerpo Nacional de Policía[708] establece en su jerarquía la Brigada de Investigación Tecnológica (BIT)[709] cuya función es "responder a los retos que plantean las nuevas formas de delincuencia. Pornografía infantil, estafas y fraudes por Internet, fraudes en el uso de las comunicaciones, ataques cibernéticos, piratería..."[710]. La Guardia Civil, en su estructura[711] y de forma análoga cuenta con el Grupo de Delitos Telemáticos (GDT)[712] competente en la investigación "que alcanza a todas aquellas conductas delictivas realizadas a través de los sistemas de información o contra éstos, lo que se conoce popularmente como el cibercrimen"[713]. Es decir, tanto la BIT como el GDT tienen como función proveer de la seguridad pública[714] necesaria para el ejercicio de lo que podríamos denominar "las libertades informáticas", lo que nos da una idea tanto de la autonomía -que no independencia- de esta libertad respecto de otras, como de la relevancia asignada por el Estado a este campo.

En todo caso, lo cierto es que el único precepto constitucional que menciona expresamente a la informática es el artículo 18.4 CE, que señala que "la ley limitará el uso de la informática" con el fin de garantizar el honor y la intimidad personal y familiar de los ciudadanos, y más importante que ello, el pleno ejercicio de sus

[708] Real Decreto 400/2012, de 17 de febrero, por el que se desarrolla la estructura orgánica básica del Ministerio del Interior.

[709] La BIT pertenece a la Unidad Central de Delincuencia Económica y Fiscal (UDEF Central), enmarcada bajo la Comisaria General de Policía Judicial. Una breve reseña en LÓPEZ, A.: "La investigación…" ob. cit. p. 67 y FERNÁNDEZ LÁZARO, F.: "La Brigada…" ob. cit. pp. 133 y ss.

[710] Página web de la BIT: http://www.policia.es/org_central/judicial/udef/bit_quienes_somos.html

[711] Real Decreto 400/2012, de 17 de febrero, por el que se desarrolla la estructura orgánica básica del Ministerio del Interior.

[712] El GDT pertenece a la Unidad Central Operativa, dentro de la Jefatura de Policia Judicial, bajo la Dirección Adjunta Operativa de la Guardia Civil. Sobre su labor, expresada por el ex jefe del órgano (2000-2011), se puede ver SALOM CLOTET, J.: "Delito…" ob. cit. pp. 103 y ss.

[713] Página web del GDT: https://www.gdt.guardiacivil.es/webgdt/home_alerta.php

[714] Denominación que acuñó el Tribunal Constitucional en la STC 104/1989, de 8 de junio.

derechos a éstos[715]. La ubicación y redacción de este precepto en nuestra Constitución genera dudas en cuanto a los límites a los que se refiere al establecer que la ley regulará el uso de la informática. Si se está hablando en todo caso de garantizar el honor, la intimidad, las relaciones familiares y otros derechos análogos, o si cuando se refiere a "pleno ejercicio de los derechos" debe entenderse cualquier otro derecho. A este respecto se ha manifestado la doctrina al vincular el artículo 18.4 CE con el artículo 197 CP en su plano tecnológico[716], y se ha llegado incluso a utilizar la expresión de libertad informática, vinculada la autodeterminación informática -no siempre referidas exactamente a la misma idea- sobre la idea de la protección en el tratamiento informático de datos personales[717]. Está idea de libertad informática, con la que nuestra posición es coincidente, no agota, en todo caso, el sentido de la libertad informática entendida como la libertad de utilizar los sistemas de información para el completo desarrollado de la persona, sino que es una parte integrante de la misma.

En todo caso, puede preverse el valor constitucional que tiene la utilización de la informática, aunque posiblemente los usos y peligros que sobre ella se ciernen hayan sido sobradamente excedidos respecto de lo que pudo suponer nuestro constituyente.

---

[715] En un sentido limitado lo ha entendido parte de la doctrina, DE ESTEBAN ALONSO, J. y GONZÁLEZ-TREVIJANO SÁNCHEZ, P.: *Tratado*… ob. cit. pp. 124. En nuestra opinión, aceptando la idea de que su ubicación no es la más adecuada, debemos apoyar la idea de que la Constitución se refiere, por un lado a la ley en sentido general (ley penal, civil, etc.), y por otro, que los ejercicios que debe garantizar con la limitación del uso de la informática son todos los existentes y no sólo los relativos al honor, la intimidad, y las relaciones familiares. En este sentido existen voces novedosas que pretenden una visión más amplia de dicho precepto constitucional, ADÁN DEL RÍO, C.: "La persecución…" ob. cit. p. 153, "aunque el acento se coloque en garantizar la intimidad, se está reconociendo la dificultad de delimitar todos los bienes jurídicos afectados, por lo que el texto constitucional en realidad ha extendido la protección a todos los derechos", también HERRÁN ORTIZ, A. I.: *El Derecho a la intimidad en la nueva ley orgánica de protección de datos personales*, Ed. Dykinson, 1ª edición, 2002, Madrid, p.99 y ss. En realidad siguen la pauta abierta mucho tiempo atrás en PÉREZ LUÑO, A. E.: "La protección de la intimidad frente a la informática en la Constitución española de 1978" en *Revista de Estudios Políticos*, nº 9, 1979, pp. 59 y ss.

[716] REQUEJO NAVEROS, M. T.: *El Delito de Revelación de Secreto Médico y la Protección Penal de la Información Genética*, Ed. Colex, 1ª edición, Madrid, 2006, pp. 32 y ss.

[717] HUERTA TOCILDO, S. y ANDRÉS DOMÍNGUEZ, C.: "Intimidad e informática" en *Revista de Derecho penal*, nº 6, 2002, pp. 16 y ss., señalan, además, que "como hemos visto, el propio Tribunal Constitucional parece avalar esta tesis diferenciadora al considerar que la llamada "libertad informática" es un "derecho autónomo" (SSTC 11/1998 y 30/1999) dirigido a controlar el flujo de informaciones relativas a uno mismo aunque no pertenezcan al ámbito más estricto de la intimidad".

Por último, también se ha tratado de relacionar la seguridad en los sistemas de información con el ámbito de protección constitucional desde el ámbito del artículo 20.1.d de la Constitución, en el que siguiendo la Declaración Universal de Derechos Humanos[718], se reconoce el derecho "a comunicar o recibir libremente información veraz por cualquier medio de difusión", de tal manera que, como se señala en la Declaración de Ginebra de 2003, tal derecho deba revisarse en favor de la realidad tecnológica a la que nos enfrentamos hoy en día[719], y adquiera especial relevancia la protección de los sistemas informáticos que permiten el desarrollo de este derecho universal[720].

Por tanto, y como ya se ha señalado, la aparición de la informática en nuestra Constitución es, directa o indirectamente, recurrente. De todo ello, creemos que podemos responder afirmativamente a la pregunta sobre si es adecuada la inclusión de la libertad de utilización de sistemas informáticos, y la seguridad que el Estado debe proveer para ello, como un valor constitucionalmente protegido; cuestión fundamental para continuar con la búsqueda de un bien jurídico relacionado con los sistemas de información. Por otro lado, a la pregunta sobre si la vulneración de este posible bien colectivo de la seguridad informática puede suponer una afectación sobre el individuo y el desarrollo de su personalidad y su desenvolvimiento en la sociedad actual, creemos que se debe responder de manera totalmente afirmativa. En España -así como en otros países de nuestro entorno- la utilización masiva de tecnología y sistemas informáticos de forma individual por los ciudadanos es máxima, no se trata de una forma de ocio en ningún caso, sino realmente un uso social completo en todos los ámbitos del desarrollo de la individualidad del sujeto (laboral, contractual, administrativo, cultural, médico, etc.). Así, el interés colectivo

[718] Artículo 19 de la DUDH establece el derecho universal recibir y difundir información, sin limitaciones y por cualquier medio de expresión.

[719] COTINO HUESO, L.: *Libertad en Internet. La red y las libertades de expresión e información,* Ed. Tirant lo Blanch, 1ª edición, Valencia, 2007, p. 58.

[720] Sobre la vinculación de la protección del derecho a la información y la seguridad informática se manifiesta COTINO HUESO, L.: *Libertad…* ob. cit. pp. 76 y ss., al inclinarse por entroncar la defensa de los sistemas de información con la libertad de expresión e información, al ser estos "cauces superdesarrollados" de transmitir y difundir información. Por lo tanto, velar por la seguridad de los mismos se convierte en una obligación pública, que debe destinar de cuantos medios disponga (se entiende, por tanto, también el Derecho penal) a este fin.

trasciende del mero interés "de la mayoría", al suponer su vulneración la producción de un daño en esferas propias de cada individuo.

Por último, la construcción del bien jurídico exige que el riesgo sobre el mismo sea real para justificar la creación de los tipos penales destinados a protegerlo. En nuestra opinión, este punto es el menos discutible de esta parte de la investigación. El peligro real de ataques sobre sistemas de información no sólo es un riesgo, es una realidad[721]. Si existe una característica constatable en nuestro Derecho penal en relación con los delitos informáticos es que su aparición ha sido muy posterior a éstos, y ya son bien conocidos no sólo los riesgos, sino los posibles efectos de las acciones delictivas.

Precisamente la relevancia del riesgo para la aceptación del bien jurídico característico de los delitos informáticos, radica en otro ámbito. La intensidad del riesgo sobre el bien jurídico va a ser uno de los elementos más relevantes a la hora de hacer una selección adecuada de los tipos penales que integran la protección del mismo; en efecto, tal riesgo no se manifestará con la misma intensidad en los delitos de daños informáticos, que en los de estafa informática, o en los delitos relativos al contenido (pornografía infantil o propiedad intelectual); pues no en todos ellos aparecerá un riesgo para el bien jurídico de entidad suficiente, y por lo tanto su ubicación sistemática en el Código deberá mantenerse inalterada incluso aceptando la necesidad de incluir un nuevo Título relativo a los delitos informáticos. En ciertos delitos informáticos, el bien jurídico protegido principal no será el relacionado con la seguridad informática, sino con los ya existentes, siendo en todo caso este nuevo bien el afectado de forma secundaria. Al contrario, algunos tipos penales, como veremos, tendrán como objeto primordial la defensa de esta seguridad informática, y de forma secundaria, la protección de otros bienes jurídicos también relevantes[722].

[721] Ya constatamos las dificultades en la prevención de este tipo de delitos, y en la comisión habitual de acciones destinadas a afectar la seguridad de la informática.

[722] GALÁN MUÑOZ, A.: "Expansión…" ob. cit. p. 23, señala con razón que "este concepto [criminalidad informática] se delimita atendiendo al hecho de que todos los delitos que se incluyen en su seno afectarían a un bien jurídico colectivo común, con independencia del concreto valor individual que también se pudiese lesionar o poner en peligro por tal conducta".

a.2. La seguridad informática desde otras ópticas dogmáticas.

En todo caso, no debemos olvidar que la existencia de un bien jurídico protegido como forma de legitimación del Derecho penal no es única, y aunque sí es mayoritaria, y por ello su desarrollo ocupa un lugar prioritario en nuestra investigación, parece adecuado enfocar la legitimación de la existencia de los delitos informáticos desde otras ópticas, para concluir si tal variación en la teoría de legitimación del derecho penal, y por ende, de los propios delitos informáticos como tipos autónomos, se ve sustancialmente alterada.

En los últimos tiempos, y cada vez con mayor intensidad, se ha venido expresando la necesidad de superar las limitaciones que supone encomendar a la protección de bienes jurídicos relevantes la legitimación necesaria para la aparición de Derecho penal, especialmente cuando desde la perspectiva clásica de protección del individuo se pretende hacer válida esa misma teoría para bienes jurídicos colectivos[723]. Así, se han planteado otros modelos que no son nuevos, sino que evolucionan de otros anteriores, cuya pretensión es justificar la aparición del Derecho penal con base en otros principios[724]. Precisamente en nuestra construcción dogmática de los delitos informáticos estamos señalando que nos encontramos ante bienes jurídicos colectivos (la seguridad en los sistemas de información, o la seguridad informática), que si bien afectan a la libertad del individuo, no podemos sino plantearlo como bienes colectivos por su naturaleza obvia. Estas fórmulas, en el extremo que ahora interesa, no vienen sino a acentuar la necesidad de protección penal de estos bienes colectivos, y aunque lo hacen, es cierto, desde la crítica de la teoría del bien jurídico protegido, no es su intención sino la de completar ésta en lo

[723] STRATENWERTH, G.: "La criminalización en los delitos contra bienes jurídicos colectivos" en HEFENDEHL, R.: *La teoría del bien jurídico ¿Fundamento de legitimación del Derecho penal o juego de abalorios dogmáticos?*, Ed. Marcial Pons, 1ª edición, Madrid, 2007, pp. 371 y 372.

[724] Modelo de reconocimiento recíproco, SEELMANN, K.: "El concepto de bien jurídico, el *harm principle* y el modelo del reconocimiento como criterios de merecimiento de la pena" en HEFENDEHL, R.: *La teoría del bien jurídico ¿Fundamento de legitimación del Derecho penal o juego de abalorios dogmáticos?*, Ed. Marcial Pons, 1ª edición, Madrid, 2007, pp. 373 y ss., se trata de dar respuesta, una vez más, al problema que siguen planteando los bienes jurídicos colectivos con la concepción clásica del bien jurídico vinculado a los derechos subjetivos. Desde una perspectiva *hegeliana* se señala la creación de un modelo que permite reunir pacíficamente el derecho subjetivo y la norma positiva en forma de relación recíproca.

que no alcanza. En este ámbito de búsqueda de justificación alternativa se mueve la legitimación material del Derecho penal desde un punto de vista utilitarista que supone (igualmente) un ejemplo claro de cómo la visión de los delitos contra la seguridad en los sistemas de información puede verse reforzada desde otras ópticas dogmáticas. Desde esta concepción, dicha legitimación previene de la necesidad de garantizar la vigencia de una serie de expectativas esenciales de la sociedad, y en la que precisamente se señala, muy en relación con los delitos de nuestro estudio, que la concepción del bien jurídico "no se ajusta a aquellas normas que deben proteger directamente la paz social sin pasar por la protección de bienes" [725].

En las siguientes páginas intentaremos configurar las acciones delictivas relativas a los sistemas informáticos como supuestos de lesión de la paz social por un lado, y contra la colectividad por otro. Por ello, aunque su relevancia para nuestro estudio es menor, cabe señalar que otras propuestas dogmáticas -tanto si buscan mejorar la teoría del bien jurídico protegido como si la descartan en favor de otra forma de fundamentar el Derecho penal- lejos de complicar la existencia de nuestra tesis, la apoyan sustancialmente, más allá del posterior trabajo, de reconocer la libertad o seguridad informática como un valor colectivo superior de la sociedad.

Podríamos concluir, por tanto, que otras concepciones que excluyen la relevancia del bien jurídico protegido como fuente de legitimación del Derecho penal no suponen nuevas o importantes dificultades sistemáticas en cuanto a justificar la existencia de los delitos contra los sistemas de información sino, en todo caso, incluso podría señalarse que fortalecen su posición y existencia en el actual ordenamiento jurídico penal.

B) CONSTRUCCIÓN DEL BIEN JURÍDICO PROTEGIDO EN LOS DELITOS INFORMÁTICOS: LA SEGURIDAD EN LOS SISTEMAS DE INFORMACIÓN

En la actualidad debemos entender que nuestro Derecho penal no consagra un bien jurídico protegido relacionado con la informática o los sistemas de

[725] JAKOBS, G.: *Derecho*… ob. cit. p. 54.

telecomunicaciones[726]. En principio todos los delitos informáticos en sentido amplio protegen bienes jurídicos diversos. El delito de acceso ilícito regulado en el artículo 197.3 CP se encuentra ubicado en los delitos de revelación de secretos, lo que indica el bien jurídico protegido es la intimidad. El delito de estafa informática del artículo 248.2.a CP o los actuales daños informáticos (264 CP) protegen el bien jurídico patrimonio, la falsedad informática (donde se protege la seguridad en el tráfico jurídico[727]) o los delitos relativos al contenido (propiedad intelectual o pornografía infantil) en los que se protege el derecho patrimonial que el autor tiene sobre su creación literaria, artística o científica (artículos 273 a 277 CP)[728] y por otro lado la seguridad del menor o su derecho a la propia imagen (artículo 189 CP)[729].

Se deduce por tanto que el Código penal español no establece la existencia de un bien jurídico vinculado a la informática que merezca protección, y en el momento actual en el que nos encontramos, en el que los sistemas informáticos han copado absolutamente todas las facetas de la vida en la sociedad, cabría, al menos, preguntarse si eso es o no es correcto[730], y en su caso tratar de definir ese bien

[726] MATA y MARTÍN, R. M.: "Criminalidad…" ob. cit. p. 34, expone sustancialmente esta visión negativa sobre la existencia de un bien jurídico inherente a la informática cuando determina que lo importante para que una actividad informática deba ser entendida como delictiva es que se pueda vincular a un bien jurídico preexistente manifestado por el legislador.

[727] Debemos entenderlo en su sentido más amplio, pues partiendo de las interpretaciones del Tribunal Supremo encontramos muy diversas concreciones del bien sobre las que ahora no interesa debatir. La STS de 27 de mayo de 1988 establece que el objeto de protección es "el ataque a la fe pública o a la confianza de la sociedad en el valor probatorio de los documentos. En otras sentencias se hace referencia a bienes similares, SSTS de 13 de diciembre de 1990, de 27 de junio de 1991, de 27 de abril de 1992.

[728] Cuestión pacífica tanto en la doctrina como en la jurisprudencia. QUINTANO RIPOLLÉS, A.: *Tratado de la Parte especial de Derecho penal*, tomo III, Ed. Revista Derecho Privado, 2ª edición, Madrid, 1978, p. 658, RODRÍGUEZ RAMOS, L: "Protección penal de la propiedad industrial" en VVAA: *Propiedad Industrial teoría y práctica*, Ed. Editorial Centro de Estudios Ramón Areces, 1ª edición, Madrid, 2001, p. 361 o BAJO FERNÁNDEZ, M. y BACIGALUPO SAGGESE, S.: *Derecho penal económico*, Ed. Editorial Universitaria Ramón Areces, 2ª edición, Madrid, 2010, pp. 482 y 483; también STS 1479/2000, de 22 de septiembre. Aunque BERDUGO GÓMEZ DE LA TORRE, I.: "La reforma de los delitos contra la propiedad industrial" en *Documentación Jurídica*, nº 37-40, 1985, p. 740, entendía que debe observarse un bien supraindividual.

[729] Doctrina que procede de la STS 22 de junio de 2010, en la que modificaba su anterior criterio, en el que señalaba que el bien jurídico protegido era "la libertad o indemnidad sexual del menor".

[730] Tal lógica evolución ya se señala a mediados de la década de los años noventa en PÉREZ LUÑO, A. E.: *Manual de informárica y derecho*, Ed. Ariel, 1ª edición, 1996, Barcelona, p. 70.

jurídico digno de protección relacionado con los sistemas informáticos, así como analizarlo convenientemente para resolver las incógnitas subyacentes.

b.1. La seguridad en los sistemas de información como bien jurídico digno de protección penal.

Comenzando con el análisis de los instrumentos internacionales más relevantes, es decir, el Convenio de 2001 y la Decisión Marco de 2005, debemos señalar que si bien el concepto de bien jurídico no aparece en sus diversas exposiciones de motivos, sí hacen referencia a la trascendencia de los sistemas informáticos en la sociedad actual, y la necesidad de su protección. El Convenio sobre la Ciberdelincuencia de Budapest de 2001 señala en su preámbulo como uno de los motivos que lo originan "los profundos cambios provocados por la digitalización, la convergencia y la globalización continua de las redes informáticas". Pero en lo que ahora nos interesa, es muy importante la vinculación de estos cambios con el mantenimiento del nivel de libertad de los individuos al señalar la necesidad de garantizar "la libertad de expresión, que comprende la libertad de buscar, obtener y comunicar información e ideas de todo tipo, sin consideración de fronteras, así como el respeto de la intimidad", lo que da buena cuenta del nexo, ya señalado en esta investigación, de la aparición de una posible libertad informática, como manifestación de la libertad clásica. Sin embargo, aparte de estas menciones, pronto comienza el articulado del mismo sin hacer más puntualizaciones a este respecto. En cuanto a la Decisión Marco 2005/222/JAI del Consejo, se expresa en una línea similar, algo más detallada, en la que se pone de manifiesto la vinculación de estos ataques contra sistemas informáticos con objetivos terroristas, al haberse convertido las infraestructuras de la información en elementos vitales de los Estados, y así expresa que "esto pone en peligro la realización de una sociedad de la información segura y de un espacio de libertad, seguridad y justicia, y por tanto exige una respuesta por parte de la Unión Europea" justificando así la regulación penal aprobada[731]. No se puede afirmar que desde los organismos internacionales se esté aceptando la existencia de un nuevo bien jurídico superior. Sin embargo, atendiendo

[731] SÁNCHEZ MEDERO, G.: "Internet…" ob. cit. (edición electrónica sin numerar), establece la relación entre el paso de la ciberdelincuencia hacia el ciberterrorismo trazando una como la evolución de la otra.

a su enunciado, especialmente en la Decisión Marco, parece quedar suficientemente acreditado que la seguridad informática que se propugna con la regulación se basa en la protección de la libertad informática, que sí queda reconocida. En esta línea sigue la evolución europea del problema, ya que en la proposición de Directiva para sustituir la actual Decisión Marco se hace hincapié en su provisional preámbulo que alguna de las acciones contra los sistemas informáticos "puede por sí sola constituir un grave peligro para el interés público"[732]. Podemos por tanto confirmar la tendencia a incardinar la relevancia de la seguridad de los sistemas informáticos tanto en la libertad individual de los ciudadanos, como en la protección de valores colectivos de la sociedad. Lo que convierte a la propia seguridad informática en un elemento de peso considerable en la configuración de una sociedad segura y libre.

Por su parte, el legislador español, en la exposición de motivos de la LO 5/2010 de 22 de junio, de reforma del Código penal, excluye toda posible concepción de un nuevo bien jurídico al señalar en el preámbulo de la ley de reforma que "se ha resuelto incardinar las conductas punibles en dos apartados diferentes, al tratarse de bienes jurídicos diversos"[733]. No parece caber interpretación al respecto, aunque también es cierto que la exposición de motivos, en lo relativo a estos aspectos, brilla por su brevedad y simplicidad, al limitarse a señalar que tal modificación se debe a la imposición Europea (ni si quiera menciona, a nuestro entender por olvido o falta de previsión, el Convenio sobre la Ciberdelincuencia de 2001) y parece desprenderse del escaso interés mostrado tanto en fase prelegislativa, como legislativa, que abrir un debate doctrinal sobre la conveniencia de la ubicación de estos delitos y la posible existencia de un nuevo bien jurídico no era en ningún caso prioritario[734]. De ello se resuelve hacer la transposición desde un ámbito de literalidad, sin entrar en otros

[732] FERNÁNDEZ FERNÁNDEZ, C.: "Delitos…" ob. cit. p. 15, señala como ejemplo que "uno de los motivos que está parando el crecimiento del comercio electrónico es la desconfianza debido a la inseguridad de los consumidores que no se "fían" de utilizar la red para realizar las compras de una forma más cómoda, como puede ser desde casa sin tener que desplazarse, hablamos de la seguridad técnica en el pago electrónico".

[733] Preámbulo de la LO 5/2010, de 22 de junio, Apartado XIV.

[734] URBANO CASTRILLO, E.: "Los delitos…" ob. cit. p. 18. También en URBANO CASTRILLO, E.: "Infracciones…" ob. cit. p. 155, ya se señala que "no parece discutible que el mundo de la informática y de las nuevas tecnologías, requiere un tratamiento jurídico propio, penal incluido […] La inexistencia de un apartado concreto sobre "delitos informáticos", es un hecho. Sin embargo, parece defendible que existiera, dada la especificidad de estas conductas"

debates, lo que desde un punto de política legislativa puede entenderse por la amplitud de la reforma penal llevada a cabo en 2010, pero que no debe ser óbice para que no se plantee en un futuro este debate.

Por tanto, entre la velada referencia a un posible bien jurídico relacionado con los sistemas informáticos, y la negativa visión a este respecto de nuestro legislador, debemos señalar que nuestra posición no sólo está de acuerdo con aquello que se intuye desde el ámbito internacional, sino que va a más allá de éste, al afirmar la existencia de este bien jurídico, no compartiéndose, por tanto, desde el prisma de esta investigación, la visión simplista del legislador español[735].

Ya hemos señalado al hacer el estudio de la teoría del bien jurídico que, si bien la discusión doctrinal sobre éste no es pacífica, no cabe duda de que las premisas principales existen: la vinculación a la Constitución, a través de la libertad y la seguridad, no sólo es una cuestión interpretativa, sino que en la normativa internacional queda recogida explícitamente. Y de esta importante manifestación se puede deducir la obvia influencia de la afectación de estos derechos de libertad y seguridad en la esfera personal, aún a pesar de encontrarnos ante un peligro presentado de forma colectiva. El riesgo de vulnerar este posible bien jurídico, al igual que su vinculación constitucional, queda de nuevo manifestado en la normativa internacional, pues el Convenio de 2001 lo recoge explícitamente al señalar como motivo de la aprobación del mismo "el riesgo de que las redes informáticas y la información electrónica sean utilizadas igualmente para cometer delitos"[736], pero más

[735] En esta línea se manifiesta MORILLAS CUEVA, L.: "Nuevas tendencias del Derecho Penal: Una reflexión dirigida a la cibercriminalidad" en *Cuadernos de política criminal*, nº 94, 2008, pp. 18 y ss., se refiere a la "aparición de modernos bienes jurídicos y del surgimiento de nuevos riesgos". También AROCENA, G. A.: "De los Delitos Informáticos" en *Revista de la Facultad de Derecho UNC*, vol. 5, nº 1, 1997, pp. 44 y ss. y DÍAZ GÓMEZ, A.: "El delito…" ob. cit. pp. 181 y ss. En palabras de éste último "cualquier solución pasa por una visión conjunta de todos ellos. Son pues las peculiaridades que plantean los nuevos delitos las que justifican su análisis particular; luego es necesario agrupar los tipos con rasgos y problemas comunes para un tratamiento adecuado y armonioso […] La autonomía de los delitos informáticos debe ser afianzada y desligada de los tipos comisivos tradicionales. Ello por una razón tanto teórica (si bien las modalidades comisivas informáticas pueden asociarse a tipos ya existentes, la función de las nuevas figuras delictuales sería la protección de la información y no del bien jurídico tradicional), como funcional (garantizar una adecuada persecución de estas conductas).

[736] DE LA MATA BARRANCO, N. J, y HERNÁNDEZ DÍAZ, L.: "El delito…" ob. cit. p. 329, señalan que según pretende afirmar el Convenio "no se trata de entender que se protege la información contenida en soportes informáticos porque tenga más valor en sí misma que otra información

allá va, si cabe, la Decisión de 2005, en la que, amén de utilizar la palabra "peligro"[737] en lugar de riesgo, señala que "se ha comprobado la existencia de ataques contra los sistemas de información […]" lo que supone hablar no ya de riesgo, sino de la concreción de ese riesgo en acciones que ponen en peligro la libertad y seguridad en los sistemas de información.

De todo lo expuesto, creemos correcto afirmar que existe dicho bien jurídico relativo a los sistemas de información, y que su formulación más adecuada sería la de "**seguridad en los sistemas de información**"[738], nomenclatura que hemos venido utilizando de forma abstracta y que a continuación trataremos de delimitar. Esta posición, aunque contraria al criterio del legislador nacional, parece ser respaldada mayoritariamente, al menos en su concepción general, por la doctrina más moderna[739].

---

contenida en otros soportes, pero sí que ello se hace por la importancia que tiene individual y socialmente su integridad y accesibilidad al estar situada en redes o sistemas informáticos de los que hoy en día dependen todos los ámbitos públicos y privados, más allá del daño al dato o sistema concretos".

[737] "Esto pone en peligro la realización de una sociedad de la información segura y de un espacio de libertad, seguridad y justicia". También utiliza la palabra "amenaza" con el mismo significado: "para responder con eficacia a esas amenazas es necesario un planteamiento global en materia de seguridad de las redes y de la información […]."

[738] Se sigue la tesis de GALÁN MUÑOZ, A.: "Expansión…" ob. cit. p. 23, que determina que "el injusto típico de estos nuevos delitos se configura atendiendo a la afectación de un bien jurídico colectivo e institucional de perfiles poco definidos: La seguridad y la confidencialidad de los sistemas informáticos". Cercana a esa línea sobre la seguridad informática como núcleo de protección se manifiesta ADÁN DEL RÍO, C.: "La persecución…" ob. cit. p. 156, cuando señala que "se puede desarrollar y potenciar el reconocimiento de un nuevo grupo de delitos autónomos en el Código Penal, que tengan en cuenta principios nuevos, una suerte de seguridad o de privacidad informática o de otro modo, pero que no dependan en su interpretación del ámbito patrimonial o de la intimidad o cualesquiera otros bienes jurídicos tradicionales".

[739] Entendemos que el reconocimiento de este nuevo bien jurídico de ámbito colectivo responde a las dudas planteadas por la doctrina, que ha ido aceptando en los últimos años la dualidad entre delitos informáticos en sentido abstracto (todos aquellos en los que aparecen elementos informáticos, y que pueden ser eventualmente, cualquier delito tradicional) y delitos informáticos en sentido estricto (aquellos en los que el objeto material del delito es el propio sistema informático o sus elementos lógicos, y cuya aparición en el Código es escasa y muy determinada). A favor de contemplar la posibilidad de la existencia de un nuevo bien jurídico protegido de tratamiento autónomo que afecta a un reducido número de tipos penales se muestran: REYNA ALFARO, L. M.: "La criminalidad…" ob. cit. p. 545, URBANO CASTRILLO, E.: "Infracciones…" ob. cit. pp. 155 y 156, "otra razón que aconsejan ese tratamiento separado y especifico de la criminalidad informática, es su incidencia en las categorías y conceptos jurídicos clásicos", NAVA GARCÉS, A. E.: *Delitos informáticos*, Ed. Editorial Porrúa, 2ª

b.2. Delitos informáticos que integran el nuevo bien jurídico protegido.

Podemos señalar que, si bien desde nuestra posición es correcta la creencia en la existencia de un valor superior merecedor de protección penal, que además es de primer orden y refleja valores constitucionales tal y como se ha desarrollado la sociedad y que posee las características de ser sustancialmente autónomo, general y colectivo, dicho valor ni es inequívoco ni se han fijado por ahora unos límites al mismo. Por ello, es ahora momento de tratar de acotar ese bien jurídico digno de protección, y con base en el mismo, analizar si existe, y con qué intensidad, en los diferentes tipos de delitos informáticos señalados en el ámbito internacional[740].

---

edición, México D.F., 2007, p. 97, señala que "cabe destacar que los delitos informáticos [refiriéndoseme exclusivamente a los delitos de acceso ilícito, daño y sabotaje informático y estafa informática] van más allá de una simple violación a los derechos patrimoniales de las víctimas", ROVIRA DEL CANTO, E.: *Delincuencia informática*… ob. cit. p. 69, "no puede partirse ya de la base de configurar el delito informático únicamente sobre el bien o interés jurídico tradicional afectado", BARRIO ANDRÉS, M.: "La ciberdelincuencia…" ob. cit. p. 278, "ahora bien, los delincuentes han encontrado en Internet un campo especialmente abonado para la comisión de delitos, lo que exige una respuesta penal específica a estas conductas" para luego señalar como delitos de esta respuesta penal especifica los delitos relacionados con la pornografía infantil, el acceso ilícito y la causación de daños, MAZA MARTÍN, J. M.: "La necesaria reforma del Código Penal en materia de Delincuencia Informática" en *Estudios Jurídicos. Ministerio Fiscal*, nº 2, 2003, p. 299, concluye en su estudio sobre el sabotaje informático en "la conveniencia del tratamiento independiente y separado del sabotaje informático respecto del delito de daños, máxime cuando en este, se protege exclusivamente el patrimonio de un tercero, a diferencia del carácter pluriofensivo de aquel, que se refiere también a otros intereses económicos distintos del meramente patrimonial"; en sentido similar también, ÁLVAREZ VIZCAYA, M.: "Consideraciones…" ob. cit. p. 277, ANDRÉS DOMÍNGUEZ A. C.: "Los daños informáticos en la Unión Europea" en *La Ley: Revista jurídica española de doctrina, jurisprudencia y bibliografía*, nº 1, 1999, pp. 1726 y ss., o RODRÍGUEZ MOURULLO, G.; LASCURAIN SÁNCHEZ, J. A. y ALONSO GALLO, J.: *Derecho*…" ob. cit. pp. 280 y ss. En contra: MATELLANES RODRÍGUEZ, N.: "Algunas…" ob. cit. p. 132, se posiciona a favor de la actual regulación a través de las figuras típicas tradicionales al señalar que la protección de los intereses patrimoniales "se pueda[e] seguir ofreciendo desde tipos penales no específicamente informáticos", MATA y MARTÍN, R. M.: *Delincuencia*... ob. cit. pp. 63 y ss. o GUTIÉRREZ FRANCÉS, M. L.: "Reflexiones…" ob. cit. p. 90, para quien "la utilización pervertida y abusiva de las altas tecnologías en la dinámica comisiva de un hecho ilícito no cambia la naturaleza de éste (el delito seguirá siendo, por ejemplo, una estafa, o un delito de falsedad documental, o de blanqueo de capitales o fraude fiscal…)"; aunque es cierto que la misma autora ha manifestado en GUTIÉRREZ FRANCÉS, M. L.: "Reflexiones…" ob. cit. p. 71, que "es hora de replantearse si tiene sentido seguir abordando esta materia como algo excepcional". Con dudas GALLARDO RUEDA, A.: "Delincuencia…" ob. cit. p. 373, "cierto es que la estafa, el robo de información, la copia ilegal, la apología del terrorismo, de la pornografía y de la violencia, la invasión ilícita de la intimidad… son delitos de siempre. Pero también es cierto que la tecnología ha hecho posible diluir la rotundidad de conceptos como el espacio y el tiempo".

[740] URBANO CASTRILLO, E.: "Los delitos…" ob. cit. p. 18, señala que "cuando hablamos de delito informático nos referimos a un tipo de delito, ya sea tradicional o propio de la sociedad de la

Aunque el núcleo de nuestra investigación se ha desarrollado en torno a los delitos del artículo 264 CP, de daños informáticos, debemos hacer ahora una breve reflexión sobre la idoneidad o no de ubicar otros tipos penales relativos a la informática junto con los delitos del actual 264 CP.

b.2.1. Delitos en los que se manifiesta con mayor intensidad.

Como hemos señalado, la seguridad en los sistemas de información no se va a manifestar con igual intensidad en todos los delitos informáticos que nos hemos ocupado de clasificar en repetidas ocasiones a lo largo de esta investigación. Conocer cuáles de ellos integran el núcleo de los delitos contra la seguridad en los sistemas de información es esencial para poder llevar a cabo una proposición de reforma coherente.

En principio, salvo mejor criterio, deberán integrar tales delitos aquellos que ponen en peligro el correcto funcionamiento de las redes de información, así como los elementos que forman parte de las mismas. Se entiende por tanto, que aunque el bien jurídico es común, el objeto material puede diferir en los diferentes tipos penales, de forma que el grupo de estos objetos va a quedar relativamente restringido. Así, éstos se clasificarían de la siguiente manera:

a) Datos informáticos, que incluye tanto a los programas informáticos como a los documentos electrónicos. Se excluyen datos en el sentido otorgado por la LOPD[741] (datos sobre el estado civil, número de teléfono, de cuentas bancarias, etc., que en todo caso serían considerados documentos electrónicos) en tanto en cuanto no se encuentren en soporte informático (documentos electrónicos). En general, podemos usar la expresión "información informática" para referirnos a todos ellos.

b) Sistemas informáticos, que incluye tanto a ordenadores, como dispositivos de telefonía móvil, videoconsolas, equipos médicos informatizados, etc.

---

información, propiciado por las tecnologías que esta aporta", lo que deja entrever claramente que se posiciona a favor de las dos soluciones a la hora de regular los delitos informáticos en el Código, por un lado aquellos para los que bastará una simple acomodación de tipos clásicos, y por otro aquellos que por sus características especiales, y homogéneos entre ellos, deberán propiciar una regulación autónoma del resto de figuras vigentes.

[741] Ley Orgánica 15/1999 de 13 de diciembre de Protección de Datos de Carácter Personal.

c) Redes informáticas, los canales de transmisión de los datos informáticos entre sistemas informáticos, se encuentren o no en determinado momento realizando su función de canal de comunicación.

Además, cabe señalar que en este bien jurídico que planteamos no existe sólo el riesgo de su vulneración en forma de resultado (delitos de lesión), sino que existen ciertas manifestaciones que, se ha comprobado, sin llegar a producir un daño concreto, pueden poner en riesgo dicho bien con suficiente entidad como para que estas acciones deban ser igualmente incardinadas como delitos contra la seguridad en los sistema de información (delitos de peligro). Es decir, no sólo el daño concreto provoca la vulneración del bien jurídico, sino que acciones encaminadas a la perpetración del daño, pero que nada tienen que ver con él, deben ser igualmente perseguidas al menos en los casos más flagrantes. Nos referimos fundamentalmente a la creación de virus informáticos u otro software malicioso, y su difusión por las redes informáticas[742]. La entidad de estas acciones, aunque pudieran no producir daños concretos sobre las clases de objetos materiales referidos, pone manifiestamente en peligro la seguridad en los sistemas de información. Por ello, en nuestra elección de los tipos penales que integran la protección de la seguridad de los sistemas de información se encontrarán tanto delitos de resultado como delitos de peligro.

En este contexto, aunque en las siguientes páginas realizaremos una propuesta más pormenorizada, así como una propuesta de reformulación de los tipos penales que deberían quedar reunidos en torno a la protección de los sistemas de información, podemos señalar sin lugar a dudas que deben incluirse entre ellos los delitos de acceso ilícito -actual 197.3 CP- y muy estrechamente ligado el intrusismo informático -actual 256 CP-, daño informático -actual 264.1 CP-, sabotaje informático -actual 264.2 CP-, abuso de dispositivos (no regulado) y desordenes públicos en las telecomunicaciones -parcialmente, actual 560.1 CP-.

[742] Aun señalando que nos encontramos ante la posibilidad de la aparición de tipos penales de peligro, a la hora de pormenorizar nuestra propuesta legislativa señalaremos como delito de peligro abstracto tal acción.

A pesar de las diferencias obvias en cada tipo penal, todos ellos reúnen una serie de características comunes más allá del figurado bien jurídico protegido que defendemos[743]. En primer lugar existe una coincidencia sustancial entre los objetos materiales a que se refieren estos delitos -datos informáticos, sistemas informáticos y redes informáticas-, además, la comisión de estas conductas típicas, más allá de suponer un daño en sentido amplio para el sujeto propietario de los datos, el sistema o la red, va a crear una situación de desconfianza hacia la utilización de los medios informáticos en la sociedad[744]. Quebrantar la confianza en la utilización de los sistemas informáticos va suponer un daño -general- de entidad mucho mayor que el daño -concreto- efectivo que se pueda producir sobre los objetos del delito, ya suponga éste un atentado al patrimonio u otros bienes jurídicos tradicionales relevantes. Así, la hipotética situación en la que a través de un ataque informático se accede ilícitamente a los documentos almacenados en un servidor web en el que se encuentran los datos relativos a las compras realizadas por sus usuarios; mucho más allá de un posible -pero no automático- delito contra la intimidad, genera una inseguridad creada en los usuarios de sistemas y redes informáticas a continuar ejerciendo su libertad informática, en la que radica la verdadera trascendencia de la acción. No se trata de que la posible vulneración de la intimidad sea de mayor o menor entidad, debido a que posiblemente los sistemas informáticos a los que se ha accedido contengan datos de usuarios de escaso valor en relación con su intimidad, sino que, el mero hecho de tal acción crea la desconfianza en esos usuarios, que les plantea la razonable duda sobre lo acertado de utilizar sistemas informáticos en el

[743] Sigue esta idea CORCOY BIDASOLO, M.: "Problemática…" ob. cit. p. 10, al señalar que "se parte de que el buen funcionamiento de los sistemas es condición indispensable para el normal desarrollo de las relaciones económicas y personales de nuestros días, porque de ello depende que no se colapsen las actividades del mundo bancario, bursátil, de seguros, transportes, gestión tributaria, Seguridad Social, sanitario… Esta segunda posibilidad es la admitida en muchas legislaciones locales estadounidenses que tipifican, de forma autónoma, conductas de acceso ilegal a un sistema informático, su uso sin autorización y la manipulación ilícita y modificación de datos informatizados."

[744] DE LA MATA BARRANCO, N. J. y HERNÁNDEZ DÍAZ, L.: "El delito…" ob. cit. p. 330, aunque se refieren al antiguo 264.2 CP su conclusión es igualmente válida: "que los daños informáticos lesionen o pongan en peligro la confidencialidad, integridad y disponibilidad de los datos y sistema informáticos no impide que, al mismo tiempo, se vulnere la propiedad u otro tipo de intereses de carácter económico; las conductas que describe el art. 264.2 tendrían, en este sentido, carácter pluriofensivo". También RODRÍGUEZ MOURULLO, G.; LASCURAIN SÁNCHEZ, J. A. y ALONSO GALLO, J.: *Derecho*… ob. cit. pp. 261 y ss. y ROVIRA DEL CANTO, E.: *Delincuencia informática*… ob. cit. pp. 71 y ss.

futuro[745]. Puede resultar igualmente conveniente poner como ejemplo el bloqueo de una página web, en la que cientos de miles de usuarios realizan consultas diariamente. Dicha acción puede no implicar un ilícito -civil o penal- meramente patrimonial, que afecta al propietario de la web atacada, sino que va a trascender al propietario del objeto para suponer una vulneración de la seguridad y confianza de los usuarios en las redes de información. O siguiendo dentro de lo que hasta ahora se consideran delitos patrimoniales, un ataque contra los servidores de la administración pública con el fin de borrar los datos informáticos de los ordenadores en un determinado ámbito (licitaciones públicas por ejemplo) encuentra una discutida cabida como delito patrimonial[746], a pesar de que los supuestos agravados del actual artículo 264.3 CP de daños informáticos aparecen cuando se afectan "intereses esenciales" o se producen daños de "especial gravedad". En todo caso, aunque pueda existir el daño patrimonial clásico, parece claro que el bien jurídico que se encuentra principalmente vulnerado no es el patrimonio, sino la seguridad informática de los sistemas y redes informáticas. Todavía más, la mera distribución de virus informáticos, hoy en día no tipificada como delito (contraviniendo los tratados

[745] En contra de una visión de bien colectivo en la llamada "seguridad informática" se muestra GALÁN MUÑOZ, A.: "La internacionalización…" ob. cit. pp. 95 y ss., que determina que el acceso a un sistema informático ajeno sólo afecta al sistema accedido y a su legítimo usuario y no existe otra afección real de índole colectiva. Violar la seguridad de un sistema informático, en opinión del autor, no es violar la seguridad informática como valor general del ordenamiento, que es cierto, no descarta su existencia. Construye así el derecho a la inviolabilidad informática, estrechamente relacionado con la intimidad, pero sin ser exactamente igual. Nuestra posición difiere sustancialmente de este punto de vista, pues consideramos, al contrario que el autor, que la seguridad informática como bien colectivo sí se ve vulnerada con la realización de la conducta típica, en tanto en cuanto, en el acceso ilícito a un sistema informático el peligro que tal acción supone para la sociedad tiene una intensidad notablemente mayor por motivos muy diversos. El sujeto que es capaz de acceder vulnerando las medidas de seguridad de un sistema informático, puede a través de dicho acceso, proveerse de múltiples herramientas para acceder a otros sistemas, datos o producir otra serie de acciones delictivas como daños, estafas, u otros tipos penales, con una capacidad de daño sustancialmente mayor. No es un problema exclusivo del propietario de la maquina a la que se ha accedido ilegítimamente, la capacidad del sujeto de llevar a cabo tal conducta pone en peligro cualquier otro sistema informático que se encuentre conectado al anterior, que hoy en día, con la existencia de Internet, puede ser eventualmente cualquier equipo del mundo. Pero como hemos señalado, la diferente visión parte esencialmente de la consideración diferente de los bienes jurídicos tutelados, siendo la opción elegida por el legislador más cercana a la posición del autor, que a nuestra propuesta.

[746] Aunque bajo la jurisdicción francesa es ilustrativo el ejemplo aparecido en prensa hace un tiempo: "Un ataque informático a gran escala ha afectado durante semanas al Ministerio francés de Economía. El asalto[…] se centró en documentos preparativos del G20 y de otros asuntos internacionales" (EFE - 07/03/2011)

suscritos por nuestro país) no puede considerarse delictiva sino como manifestación de un atentado contra la seguridad en los sistemas de información, pues objetivamente tal acción puede provocar resultados dañinos (en ocasiones de máxima intensidad) en sistemas informáticos, lo que requiere por su relevancia, a pesar de tratarse de un mero riesgo abstracto, la intervención del Derecho penal.

En efecto, tanto en el delito de acceso ilícito del artículo 197.3 CP en el que, por su ubicación sistemática se entiende como bien jurídico protegido primordial la intimidad, como en los delitos de intrusismo informático del artículo 256 CP, muy relacionado con el anterior, pero vinculado al patrimonio; así como los daños informáticos del artículo 264 CP en los que el bien jurídico primordial se considera el patrimonio, los efectos de este tipo de acciones y el perjuicio en la sociedad que suponen distan mucho de afectar exclusivamente -e incluso principalmente- a los bienes jurídicos tradicionales protegidos en los tipos penales que los acompañan en el Código penal en la actualidad. Además de éstos, el artículo 560 CP que tipifica realmente un sabotaje informático, suponemos, de especial gravedad atendiendo a la penalidad señalada (de 1 a 5 años) por causar daños "que interrumpan, obstaculicen o destruyan líneas o instalaciones de telecomunicaciones" como manifestación de desórdenes públicos, podría ubicarse perfectamente, y con mayor facilidad al tratarse ya de un delito que protege un bien jurídico colectivo, en el catálogo de tipos penales destinados a proteger la seguridad en los sistemas de información. Por último, no debemos olvidar las acciones de abuso de dispositivos, no tipificadas en nuestro Código, que también deben ser tenidas en cuenta para una completa cobertura penal de este tipo de delincuencia.

Este listado sería por tanto el de los delitos que integrarían la protección de la seguridad en los sistemas de información y los que a la postre, como propondremos en las próximas páginas, formaran el núcleo de los delitos contra la seguridad en los sistemas de información, que deberían sufrir una reordenación en nuestro Código[747],

[747] Sobre la anterior regulación de los daños informáticos -aunque creemos extensible al resto de los delitos descrito- ya se manifestaba MARCHENA GÓMEZ, M.: *Internet…* ob. cit. p. 363 al señalar que "el día a día demuestra que esa visión [delitos en los que el interés primordial es el patrimonio de la víctima] ha sido desbordada por una realidad que impide ver en el patrimonio ajeno el único bien jurídico dañado o amenazado por la acción delictiva.

consecuencia de la cual tanto la doctrina como la jurisprudencia deberían realizar una reevaluación de su interpretación bajo este nuevo prisma.

b.2.2. Delitos en los que se manifiesta con menor intensidad.

La nota característica de los delitos anteriores es que en ellos la protección del nuevo bien jurídico establecido es prioritaria, y la protección de otros bienes jurídicos puede aparecer con diferente intensidad, pero siempre lo hará en menor medida. Por ello, aunque los anteriores forman el núcleo esencial de los delitos contra la seguridad en los sistemas de información, debemos al menos señalar cuales quedarían excluidos de tal listado, insistiendo en que el motivo no es la inexistencia de dicho bien jurídico, sino que su manifestación es, en todo caso, de menor entidad a la de otros bienes jurídicos, que podemos señalar como principales.

Básicamente el núcleo de delitos informáticos (en sentido general tal como se desprende de la normativa internacional, especialmente del Convenio sobre la Ciberdelincuencia de 2001) que quedarían excluidos de esta nueva concepción de la delincuencia informática como amenaza de la seguridad en los sistemas de información serían los de falsedad informática, los relativos a la pornografía infantil, y los atinentes a la propiedad intelectual. En todos ellos los sistemas y redes informáticas suponen la herramienta para la comisión de los ilícitos, pero tales ilícitos no pueden suponer un atentado contra la seguridad informática por encima de la lesión de los bienes jurídicos que actualmente protegen. La libertad y seguridad informática no son los bienes inmediatamente protegidos, en primer lugar porque los objetos materiales sobre los que recaen estos delitos no son medios informáticos (datos, sistemas o redes), sino documentos (que pueden o no ser informáticos), y en segundo lugar, porque la capacidad de afectación a la libertad y seguridad informática de los ciudadanos en su conjunto es mucho menor.

Más dudas suscita, a nuestro entender, el delito de estafa informática -artículo 248.2.a sobre la estafa informática y 248.2.b sobre el abuso de dispositivos en los delitos de estafa informática CP-. Por un lado, parece obvio, al igual que los anteriores, que en este caso el objeto del delito no son los medios informáticos, sino el patrimonio. Sin embargo, es igualmente cierto que su encaje en la actual

regulación de los delitos de estafa sugiere sustanciales diferencias con los elementos típicos del delito de estafa, además de requerir la tipificación del abuso de dispositivos en relación a este delito para una completa protección penal del patrimonio en la estafa, de forma similar a como es necesaria en los delitos ya seleccionados en el apartado anterior. Por otro lado, el actual desarrollo de la sociedad de la información ha contribuido a la utilización, cada vez mayor, de métodos de pago informáticos; es decir, se ha generalizado el uso de la informática para la realización de operaciones patrimoniales habituales (compra de entradas para espectáculos, compra en supermercados, contratación de seguros, compraventas entre particulares, etc.), de tal modo que la afectación del bien jurídico patrimonio en este tipo de delitos se encuentra en una posición equiparable con la afectación del bien jurídico seguridad en los sistemas de información. Desde luego la marcada aparición de afectación del bien jurídico relativo a la seguridad en los sistemas de información es de mucha mayor intensidad que en los delitos de falsedad y los relativos al contenido -pornografía infantil y propiedad intelectual- aunque es igualmente cierto que las características de la estafa informática tiende a asemejar ésta con este tipo de delitos en los que el bien jurídico protegido principal es el tradicional, antes que con los expuestos como integrantes esenciales de los delitos contra la seguridad en los sistemas de información.

Por ello, creemos adecuado mantener la tipificación de la estafa como se encuentra en la actualidad. La afectación del bien jurídico colectivo que hemos construido, puede manifestarse en todo caso, a través de la tipificación de una circunstancia agravante del tipo básico (introduciendo un nuevo apartado en el artículo 250 CP por ejemplo), en la cual se señale diferente penalidad cuando la estafa haya supuesto un peligro para la seguridad de las redes de información, quedando así recogida la lesión tanto al patrimonio, como a la seguridad en los sistemas de información[748].

[748] La estafa informática no ha sido objeto de nuestro estudio, y por ello no vamos a desarrollar esta idea de forma más detallada ahora, aunque debemos reconocer que el planteamiento propuesto establece la creación de un concepto jurídico indeterminado desaconsejable en la legislación penal que en todo caso requeriría de un estudio autónomo. Aun así, existen ideas en la doctrina sobre este planteamiento, en particular CORCOY BIDASOLO, M.: "Problemática…" ob. cit. pp. 9 y 10, señala que "para un sector doctrinal el delito informático es únicamente una forma de realización de distintos

Queda claro, por tanto, que en los delitos sobre el contenido (propiedad intelectual y pornografía infantil) y en las falsedades, no cabe entender que el bien jurídico protegido sea, al menos directamente, la seguridad en los sistemas de información, entendido desde la perspectiva del bien jurídico inmediatamente vulnerado. Con más dudas, tampoco parece lógico que sea el bien jurídico protegido principal en los delitos de estafa informática. Por el contrario, sí lo será en los delitos de acceso ilícito del artículo 197.3 CP, intrusismo informático del artículo 256 CP, de daños informáticos del artículo 264 CP, siendo especialmente apreciable en cuanto al párrafo segundo de este artículo 264 CP, así como otros delitos conexos como los desordenes públicos del artículo 560.1 CP y el abuso de dispositivos no regulado. De esta forma los delitos informáticos quedarían divididos en dos categorías generales: la primera en la que se protege fundamentalmente la seguridad en los sistemas de información, y la segunda, en la que se englobarían el resto de delitos informáticos reconocidos.

b.3. ¿La seguridad en los sistemas de información como manifestación del orden público?

Ya nos hemos manifestado en esta investigación sobre una posibilidad alternativa relativa a la naturaleza de los delitos clasificados anteriormente, en los que la seguridad en los sistemas de información puede plantearse como una categoría dependiente de otro bien jurídico reconocido en la doctrina penal. Nos referimos a la subsunción de este tipo de acciones dentro de delitos contra el orden público[749], y más concretamente como delitos de desórdenes públicos. A este respecto se ha manifestado algún autor generando a una duda razonable[750], aunque ciertamente poco se ha profundizado por esta vía dogmática.

---

tipos delictivos. En consecuencia el bien jurídico protegido en el delito informático será aquél protegido en el delito que presuntamente se ha realizado: patrimonio, Hacienda Pública… Otra concepción de la criminalidad informática le concede autonomía entendiendo que con el fraude informático se protege un bien jurídico con naturaleza propia: "*la confianza en el funcionamiento de los sistemas informatizados*" como interés de carácter supraindividual –colectivo–".

[749] Se plantea ya de partida la delimitación del concepto de orden público, que se caracteriza por su relativismo e indefinición, ARNALDO ALCUBILLA, E.: "El orden público y la seguridad ciudadana en la Constitución española de 1978" en *Cuadernos de Seguridad y Policía*, nº 7, 2011, pp. 217 y ss.

[750] MARCHENA GÓMEZ, M.: "El sabotaje…" ob. cit. pp. 353 y ss.

No cabe duda de que la legitimación del Derecho penal radica en parte en la consecución de una sociedad en paz[751]. Sin embargo, dentro del amplísimo catálogo de delitos que existen en nuestro Código penal, no todos buscan la protección directa de dicha paz social. Gráficamente, los delitos en los que se protege la integridad física de las personas, sirven para mantener la paz social, pero no es sino de forma secundaria, siendo su prioridad la protección propia de las personas que pueden sufrir atentados contra su integridad física. En cambio, el legislador ha introducido tipos penales en los que la protección primera sí se considera ese orden social, esa paz social, pero por el contrario ha excluido a los ataques contra la seguridad en los sistemas de información de éstos, salvo en una muy básica alusión que veremos a continuación.

Un ejemplo, similar a otro propuesto por la doctrina[752], y sobre el que tanto las instituciones europeas como las del resto del mundo tienen puestos los cinco sentidos, es plantear un ataque contra los sistemas de información como un ataque contra ese orden social, de tal forma que un bloqueo masivo de las infraestructuras de la información inutilice aquellos servicios que dependen de sistemas informáticos (que hoy en día son todos) de tal manera que deje fuera de servicio los transportes, la distribución de agua, de electricidad o la defensa nacional. Difícilmente podemos integrar dichos ataques informáticos en los tipos penales actuales y sólo eventualmente podrían ser coincidentes con el tipo de desórdenes públicos del artículo 560.1 CP[753] o con otros del mismo capítulo del Código. En todo caso, lo que a todas luces parece insuficiente es incardinar los mismos en tipos penales cuya máxima de protección es la intimidad (197.3 CP) o el patrimonio ajeno (264 CP), tanto desde un punto de vista sistemático y de bien jurídico protegido, como desde un punto de vista de las consecuencias jurídicas de las acciones, muy limitadas en

[751] Paz social lo denomina GARCÍA-PABLOS DE MOLINA, A.: *Introducción…* ob. cit. p. 174, o Paz pública según STRATENWERTH, G.: "La criminalización…" ob. cit. p. 370 o HÖRNLE, T.: "La protección de sentimientos en el STGB" en HEFENDEHL, R.: *La teoría del bien jurídico ¿Fundamento de legitimación del Derecho penal o juego de abalorios dogmáticos?*, Ed. Marcial Pons, 1ª edición, Madrid, 2007, p. 387.

[752] MARCHENA GÓMEZ, M.: "El sabotaje…" ob. cit. p. 363.

[753] MAZA MARTÍN, J. M.: "La necesaria…" ob. cit. p. 300, ya aventuraba la necesaria reforma de este artículo para dar cabida a la interrupción, obstaculización o destrucción de datos o sistemas informáticos.

consideración a la capacidad del daño que puede ser producido. En todo caso la solución de imputar una serie de delitos en cadena a los autores de dichos ataques siempre será una posibilidad, un concurso de delitos, previsiblemente ideal, por otra parte, del todo heterogéneo al incluirse delitos contra la intimidad, contra el patrimonio, contra el orden público, etc. o llegado el caso la posibilidad de apreciar un delito continuado[754]. La cuestión, en todo caso, es pensar si acudir a este recurso es la solución más adecuada para penalizar estas conductas o por el contrario cabría valorar la posibilidad de implantar otras soluciones, como por ejemplo, plantear la distinción entre delitos informáticos que atenten contra el orden público y delitos informáticos que vulneren otros bienes jurídicos.

Para comprender la idoneidad de este planteamiento debemos en primer lugar señalar las características de los delitos de desórdenes públicos tal como los concibe la doctrina. En nuestro sistema Constitucional, el orden público, así la como paz social, aparecen en diferentes artículos del texto citado: artículos 10.1[755] y 16.1[756]o 21.2[757], no como un Derecho sino como una situación social que el Estado está obligado a mantener y, en todo caso, como un límite al ejercicio de los derechos y

[754] MARCHENA GÓMEZ, M.: "El sabotaje…" ob. cit. pp. 364 y 365, establece que habrá que determinar, partiendo del bien jurídico protegido diferente en unas acciones y otras, en la voluntad del autor: "en aquellas ocasiones en que la causación del perjuicio económico sea el propósito que filtre la acción del sujeto activo, se estará en presencia de un delito de daños del art. 264.2 [actual 264]. Por el contrario, en aquellos otros casos en que se busque de forma deliberada la interrupción o destrozo de las comunicaciones, la aplicación del art. 560.1 resultará obligada". De esta misma opinión sobre la separación entre delitos de desórdenes públicos o tipos específicos que vulneran otros bienes jurídicos se manifiestan ESCUDERO MORATALLA, J. F., FRIGOLA VALLINA, J. y GANZENMÜLLER ROIG, C.: *Delitos contra el orden público, terrorismo, contra el Estado o la Comunidad Internacional*, Ed. Bosch, 1ª edición, Barcelona, 1998, pp. 202 y 203.

[755] Artículo 10.1 CE: "La dignidad de la persona, los derechos inviolables que le son inherentes, el libre desarrollo de la personalidad, el respeto a la ley y a los derechos de los demás son fundamento del orden político y de la paz social".

[756] Artículo 16.1 CE: "Se garantiza la libertad ideológica, religiosa y de culto de los individuos y las comunidades sin más limitación, en sus manifestaciones, que la necesaria para el mantenimiento del orden público protegido por la ley".

[757] Artículo 21.2 CE: "En los casos de reuniones en lugares de tránsito público y manifestaciones se dará comunicación previa a la autoridad, que sólo podrá prohibirlas cuando existan razones fundadas de alteración del orden público, con peligro para personas o bienes".

libertades de los ciudadanos[758], lo que habilita al legislador a la utilización de la ley penal, además de otras herramientas, para conseguir tal protección. El orden público queda así vinculado por la obligación del Estado de proveer un marco de seguridad en el que los ciudadanos puedan desarrollarse libremente[759].

En nuestro sistema penal el orden público como bien jurídico del ordenamiento digno de protección se encuentra protegido en nuestro Código penal en el Título XXII, de los delitos contra el orden público, en el que se engloban varios capítulos, siendo el de interés para nuestro estudio el tercero, de los desórdenes públicos[760], donde el bien jurídico protegido es precisamente la paz pública antes mencionada, que se vulnera con el desorden público realizado, si bien sobre la idoneidad en la utilización de estos conceptos existe discrepancia doctrinal[761], que en todo caso, no afecta al objeto de nuestra investigación.

Lo que en cambio se debe considerar de máxima importancia es si en la definición que cabría esperarse del orden público, podrían subsumirse los delitos informáticos clasificados. Si por orden público entendemos paz social, entonces, debemos señalar en la línea ya marcada, que la paz social del siglo XXI no puede

[758] Para un mayor detalle, véase BARTOLOMÉ CENZANO, J. C.: *El orden público como límite al ejercicio de los derechos y libertades*, Ed. Centro de estudios políticos y constitucionales, 1ª edición, Madrid, 2002.

[759] STC 325/1994, de 12 de diciembre, FJ. 2, señala que "ésta [la seguridad personal] a su vez, aparece conectada a la tercera especie, la seguridad pública (art. 149.1.29 C.E.) también llamada ciudadana, como equivalente a la tranquilidad en la calle. En definitiva, tal seguridad se bautizó ya en el pasado siglo con la rúbrica del orden público, que era concebido como la situación de normalidad en que se mantiene y vive un Estado, cuando se desarrollan las diversas actividades colectivas sin que se produzcan perturbaciones o conflictos. En definitiva, el normal funcionamiento de las instituciones y el libre y pacífico ejercicio de los derechos individuales". Por su parte el concepto de orden público quedó establecido de forma general por el Tribunal Supremo en la STS de 5 de abril de 1966 al señalar que el "orden público nacional está integrado por aquellos principios jurídicos, públicos y privados, políticos, económicos, morales e incluso religiosos, que son absolutamente obligatorios para la conservación del orden social de un pueblo y una época determinada", de DELGADO AGUADO J.: "El orden público: proceso evolutivo" en *Cuadernos de Seguridad y Policía,* nº 7, 2011, p. 21.

[760] En este Capítulo se enmarcan conductas dispares cuyo nexo en común es el ataque al orden público como afectación al "desenvolvimiento normal de las manifestaciones de la vida ciudadana", véase ESCUDERO MORATALLA, J. F.; FRIGOLA VALLINA, J. y GANZENMÜLLER ROIG, C.: *Delitos*… ob. cit. p. 165.

[761] La discusión entre la idoneidad de equiparar el concepto de orden público y paz pública se reproduce en ESCUDERO MORATALLA, J. F., FRIGOLA VALLINA, J. y GANZENMÜLLER ROIG, C.: *Delitos*… ob. ci. p. 166 y ss. También en BARTOLOMÉ CENZANO, J. C.: *El orden*… ob. cit. p. 270 y ss.

englobar las mismas acciones que en otros tiempos. Al igual que ciertas acciones moralmente reprochables han dejado se suponer atentados contra el orden público (principalmente relacionadas con la moralidad de la época), otras acciones, en cambio, por su reciente aparición, no deben ser excluidas como candidatas a alterar dicha paz social. En el caso de los delitos contra la seguridad en los sistemas de información podemos señalar que se encuentran tímidamente regulados en el propio Capítulo III del Título XXII sobre los delitos contra el orden público. El ya mencionado artículo 560.1 CP se redacta con cierta similitud al artículo 264.2 CP, señalando como delito la obstaculización o interrupción (mismas acciones que el artículo 264.2 CP) de líneas o instalaciones de telecomunicaciones, concepto segundo análogo al de sistemas de información[762]. Esto nos acerca a la posición de considerar que, efectivamente, las acciones que ponen en peligro los sistemas de información, pueden suponer, indudablemente, alteraciones en el orden público y que quizá lo adecuado sería, sobre la existencia del actual artículo 560.1 CP, elaborar un nuevo marco penal más desarrollado respecto de aquellas conductas que vulneran la seguridad en los sistemas de información.

Sin embargo, la subsunción de estas acciones constitutivas de delitos contra la seguridad en los sistemas de información dentro de los delitos de desórdenes públicos plantea algún problema grave. El primero y más importante, sería el derivado de aquellas conductas cuya gravedad sea menor, o cuya peligrosidad potencial sea manifiestamente reducida, pero suficientemente grave como para merecer reproche penal. Un acceso no autorizado de piratas informáticos a los ordenadores de una universidad o una pequeña (o no tan pequeña) compañía, acciones que actualmente podrían quedar subsumidas en el tipo del artículo 197.3 CP, o un ataque contra los datos y documentos electrónicos de los ordenadores de la empresa donde trabajaba un ex empleado que ha sido despedido, acción que podría ser típica según el actual artículo 264.1 CP; son acciones que difícilmente pueden ser consideradas como dignas de alterar el orden público, sin embargo, parece obvio que el legislador nacional (y el internacional) han entendido en sus líneas de política

[762] No lo es en cambio, el concepto líneas de telecomunicaciones, que pueden entenderse por las líneas de cables físicos que unen los sistemas de información (de telecomunicaciones), siendo el daño sobre estas un daño que no aparece en el artículo 264 CP, y que, en todo caso, podría suponer un daño clásico del artículo 263 CP.

criminal que deben ser acciones merecedoras de reproche penal, lo que llevaría a la necesidad de una doble tipificación en función del bien jurídico protegido. Pero sobre éste último también se ciernen dudas, ya que plantear la posibilidad de que el bien jurídico protegido principal en los delitos contra la seguridad en los sistemas de información es el orden público sufre en parte la misma crítica que sobre la situación actual se cierne, la de considerar que la seguridad en los sistemas de información siguen sin ostentar la entidad suficiente para suponer un bien digno de protección autónoma, lo que como ya hemos manifestado, no creemos que se corresponda con la realidad. Además, sería necesario un estudio del tipo subjetivo en dichas acciones, pues las conductas encaminadas a poner en peligro los sistemas de información, en función de la ubicación y forma de redacción del precepto, podrían provocar la impunidad de acciones que no vulneren, precisamente, el bien jurídico del orden público.

Por ello, aunque el planteamiento original de algún autor en este línea supone una idea bienvenida, por cuanto engloba tales conductas y las aleja de su naturaleza actual, quizá la solución no pase por incardinar los delitos contra los sistemas de información como tipos penales de desórdenes públicos, aunque nos mantenemos en la consideración de que su ubicación actual tampoco es la adecuada. Baste por ahora señalar que en una propuesta de reforma de los delitos informáticos cabría plantearse, al menos, la posibilidad de completar el artículo 560 CP, para dar cabida de la mejor forma posible a ataques contra la seguridad en los sistemas de información que sí pongan en peligro la paz social, pero no por ello excluir como conductas delictivas aquellas que no suponen una vulneración de la paz social, lo que provocaría la impunidad de acciones que el legislador ha decidido introducir en el Código. En resumen, en todo caso podría ser bienvenida la reforma de dicho artículo de forma que contemple, de alguna manera, supuestos agravados de los delitos contra la seguridad en los sistemas de información, incluso manteniendo la ubicación y

naturaleza de éstos según la actual redacción del Código, pero no sustituirlos completamente[763].

[763] De nuevo MAZA MARTÍN, J. M.: "La necesaria…" ob. cit. p. 300, también concluye que "sería conveniente la extensión del delito de desórdenes públicos (art. 560.1 CP) a la interrupción, obstaculización o destrucción".

CAPÍTULO QUINTO: PROPOSICIÓN DE UN MARCO LEGISLATIVO ALTERNATIVO PARA LOS DAÑOS INFORMÁTICOS Y DELITOS CONEXOS

1. INTRODUCCIÓN

La formulación de los tipos de daños informáticos en nuestro ordenamiento debe responder, esencialmente, a las disposiciones contenidas en el Convenio sobre la Ciberdelincuencia del Consejo de Europa de Budapest de 2001 y a la Decisión Marco 2005/22/JAI del Consejo, además de respetar, lógicamente, los principios generales de nuestra regulación penal. Creemos que aunque el objeto central de nuestra investigación son los delitos de daños informáticos, para la formulación de un marco penal alternativo una vez más nos vemos en la obligación de tratarlos como una parte de un conjunto mayor, esto es, de los delitos informáticos, según las clasificaciones internacionales.

Así, para la mejor formulación de esta nueva regulación penal somos defensores de la agrupación de los delitos informáticos en el Código penal en función del bien jurídico protegido -pues esa es la sistemática seguida por el legislador de 1995 para dar forma al Código penal-. Esto supone, en todo caso, volver sobre lo ya apuntado en las páginas precedentes al señalar que al menos tres acciones actualmente tipificadas en nuestro Código penal, y una cuarta que no se encuentra en nuestro ordenamiento pero que deberá ser introducida en el futuro por el legislador, comparten esencialmente el mismo bien jurídico principal (acceso ilícito del artículo 197.3 CP, daños informáticos del artículo 264 CP y abusos de dispositivos no regulado en nuestro ordenamiento). La naturaleza de este bien jurídico común ya ha sido discutida pero, en todo caso, supone un cambio de concepción respecto de la realidad vigente. Entender que estas cuatro infracciones protegen, primordialmente, el bien jurídico relativo a "la seguridad en los sistemas de información" supone, de entrada, la necesidad de reubicar estos tipos penales en el Código, así como dotar de un nuevo significado e interpretación a algunos de sus elementos.

2. UBICACIÓN EN EL CÓDIGO PENAL

Antes de proponer un marco legislativo alternativo al que se encuentra vigente en la actualidad, debemos detenernos en una cuestión que no ha pasado desapercibida en la doctrina ni en nuestro estudio, pero sobre la que no se ha realizado una propuesta seria y unánime al respecto, como es la de la ubicación que los delitos contra la seguridad en los sistemas de información debería ocupar en nuestro Código.

Así, el marco penal que vamos a proponer responde a un criterio de unidad de protección del mismo bien jurídico protegido, como es "la seguridad en los sistemas de información". Por ello, la regulación de los tipos penales tal y como se propone debe efectuarse, en todo caso, de una forma unitaria, bajo una misma intención protectora, y perdería sentido de producirse (como ocurre en la actualidad), una dispersión de los tipos penales en diferentes Títulos del Libro II del Código penal[764].

Siguiendo este planteamiento hemos tratado de ofrecer dos respuestas en las páginas anteriores, en las que se agrupaban los tipos penales que engloban los delitos contra la seguridad en los sistemas de información, pero desde dos ópticas diferentes. Aunque hemos visto que la doctrina ha señalado repetidamente sus dudas sobre la ubicación de los delitos de daños informáticos del artículo 264 CP como delitos de daños patrimoniales y que, incluso, se ha planteado la posibilidad de incardinar éstos en otros Títulos del Libro II del Código -desordenes públicos- está solución no ha terminado de satisfacer unos requisitos mínimos que habiliten tal posibilidad. En todo caso, ante las dudas sobre la integración del bien jurídico "seguridad en los sistemas de información" como un subconjunto de los delitos contra el orden público u otras opciones, debemos mantener la singularidad conceptual del mismo y proponer, alternativamente, la inclusión en el Libro II del Código penal de un Título independiente que regule dichas acciones. Aunque dicha reformulación supone un paso más en la concepción del bien jurídico como completamente autónomo, esta

[764] ADÁN DEL RÍO, C.: "La persecución…" ob. cit. p. 156, pone como ejemplo análogo a nuestra propuesta, la tipificación de los delitos contra la seguridad vial al manifestar que "el aumento desmedido de vehículos y sus riesgos provocaron, en su momento, el reconocimiento en el Código Penal de la seguridad vial como bien jurídico digno de protección, entendiendo el legislador que la legislación administrativa resultaba insuficiente".

calificación no puede ser descartada prematuramente. Se ha repetido en numerosas ocasiones que la relevancia de los sistemas informáticos en la sociedad actual es máxima, y la importancia de su protección no debe ser infravalorada[765].

La posibilidad de crear un nuevo Título en el Libro II no parece una proposición descabellada si atendemos a la evolución legislativa de los últimos años, a lo largo de la cual se han añadido cada vez más conductas penalmente típicas relativas a la informática que, en ocasiones, han suscitado dudas por su ubicación a la hora de ser tipificadas. Ello, además, supondrá la utilización de una mejor técnica legislativa, tanto en el presente, como para las modificaciones y ampliaciones que de este tipo de delitos deba hacerse en el futuro[766].

3. EL TÍTULO RELATIVO A LOS "DELITOS CONTRA LA SEGURIDAD EN LOS SISTEMAS DE INFORMACIÓN" Y SU CONTENIDO

Los delitos que a continuación se proponen, aglutinan esencialmente los ya tipificados en nuestra regulación penal vigente, así como los que deberían estarlo por mandato internacional, agrupados en torno a la idea de que en todos ellos, además de otros intereses y bienes secundarios, lo que se protege prioritariamente es la seguridad en los sistemas de información. Por ello, la tipificación de las conductas dentro de un mismo Título es un requisito básico para que la actual propuesta encuentre un significado pleno. Además, se hacen otra serie de modificaciones de mayor o menor intensidad dependiendo de cada caso. En todos ellos, después del

[765] ANDRÉS DOMÍNGUEZ, A. C.: "Los daños informáticos en el Derecho penal europeo" en ÁLVAREZ GARCÍA, F. J.; MANJÓN-CABEZA OLMEDA, A. y VENTURA PÜSCHEL, A. (coords.): *La adecuación del Derecho penal español al ordenamiento de la Unión Europea*, Ed. Tirant lo Blanch, 1ª edición, Valencia, 2009, p. 423, propone la creación de una Sección 2ª junto a los daños clásicos, o un nuevo Capítulo en Título XIII (modelo seguido en la legislación francesa) para dotar de absoluta autonomía a los delitos de daños informáticos. Nuestra perspectiva es que si bien dicho cambio beneficiaria la sistemática del Código, no sería suficiente, por cuanto seguiría planteando el patrimonio como bien jurídico principal digno de protección, siendo este uno de los problemas fundamentales de la cuestión.

[766] En palabras de ZUGALDÍA ESPINAR, J. M.: "¿Qué queda en pie en el Derecho penal del principio de mínima intervención, máximas garantías?" en *Cuadernos de política criminal*, nº 79, 2003, p. 109, "una intervención [del Derecho penal] distinta a la tradicional no tiene necesariamente que ser sinónimo de una intervención con menos garantías", a lo que cabría añadir que determinados cambios de concepción, realizados con tras un amplio estudio y reflexión, no sólo evitarán la disminución de las garantías, sino que redundarán en beneficio de éstas.

texto penal propuesto, se realiza una descripción del tipo, motivando las modificaciones efectuadas.

A) TIPOS BÁSICOS

a.1. Acceso ilícito.

El tipo penal quedaría redactado de la siguiente manera,

> *El que por cualquier medio y sin consentimiento, vulnerando las medidas de seguridad establecidas para impedirlo, acceda a datos o programas informáticos contenidos en un sistema informático o en parte del mismo, lo utilice, o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho a excluirlo, será castigado con pena de prisión de seis meses a un año y seis meses*.

El tipo penal coincide esencialmente con el texto actualmente regulado en el artículo 197.3 CP. En cuanto a la redacción propuesta se sustituye el concepto de autorización por el de consentimiento y por su nueva ubicación en el Código penal se produce su conversión en un delito de carácter plenamente público[767]. Se mantiene la elección anterior del legislador de penar tan sólo aquellos casos de acceso en los que es necesario vulnerar un sistema de seguridad, que es acorde a la pretensión de incluir tal tipo penal como un delito contra la seguridad de los sistemas de información[768]. A diferencia del tratamiento dogmático actual, que sitúa este tipo penal como una forma de protección anticipada de la intimidad[769] -pues parece la

[767] Con la actual regulación, este delito, con base en lo establecido en el artículo 201 CP queda tipificado como un delito privado, con algunas excepciones (afectación de intereses generales o pluralidad de personas, art. 201.2 CP).

[768] El acceso a un sistema que no tiene un sistema de seguridad carecería de trascendencia penal, al menos en el ámbito de los delitos contra la seguridad en los sistemas de información. Ello no obsta para que, en otro orden de situaciones, tal acceso pueda provocar la comisión de otros tipos penales del Código (intimidad, daño informático, etc.). Tal voluntad parece además desprenderse de la propuesta de Directiva que se presume sustituya a la Decisión Marco, en la que la vulneración de las medidas de seguridad pasa de ser un requisito opcional para el legislador nacional, a ser un requisito obligado para que se pueda apreciar el tipo penal. Sobre este tipo penal MOLINA GIMENO, F. J.: "El hacking ¿una conducta punible?" en *Diario La Ley*, nº 7131, 2009, (edición electrónica sin numerar).

[769] MIRÓ LLINARES, F.: "Delitos…" ob. cit. pp.143 y ss.

única forma de justificar su ubicación entre los delitos contra la intimidad y de revelación de secretos al estar éste exento de la característica general de apoderamiento para el descubrimiento que caracteriza los tipos penales en ese ámbito- se abandona tal consideración de protección anticipada. En efecto, el actual artículo 197.3 CP sólo se puede entender como parte de los delitos contra la intimidad en la medida en que se configure como una anticipación de las barreras de protección[770] respecto de estos delitos que se encontraban ya tipificados. No obstante, tal justificación produce a su vez efectos adversos en su interpretación: si el tipo penal es una barrera de protección anticipada en relación con los delitos contra la intimidad, ¿podemos considerar típica la acción en la que se dan todos los elementos del delito y sin embargo ellos no producen la comisión de un tipo penal contra la intimidad y sí otro como por ejemplo un daño informático?[771] En línea con lo expresado anteriormente y para dar una respuesta satisfactoria, la doctrina ha justificado la redacción del actual artículo 197.3 CP de forma tan dispar al resto de los tipos de su entorno, en la necesidad de realizar una protección de lo que ha venido a denominar abiertamente la seguridad informática[772].

Nuestra proposición, en tanto, trata de superar esta justificación y extender la protección de esta seguridad informática. Acceder ilegítimamente a un sistema ajeno vulnerando sus medidas de seguridad no sólo supone un problema potencial en cuanto a la vulneración de la intimidad o el descubrimiento de secretos. Desde nuestro punto de vista, tal acceso no implica una anticipación de las barreras de protección, sino una acción que vulnera de forma directa la seguridad en los sistemas

[770] MIRÓ LLINARES, F.: "Delitos…" ob. cit. p.144.

[771] Si es una barrera de protección anticipada en cuanto a los delitos contra la intimidad, cuyo bien jurídico protegido penalmente relevante es la intimidad, es cuestionable si acceder a un sistema de información ajeno vulnerando sus medidas de seguridad para procurarse el anonimato en un posterior delito de daños informáticos sobre un segundo sistema supondría una acción típica del 197.3 CP, por cuanto el bien jurídico penalmente relevante cuya protección anticipa, que es la intimidad del propietario del ordenador accedido, no ha sido vulnerado, conllevado la atipicidad de la conducta.

[772] MIRÓ LLINARES, F.: "Delitos…" ob. cit. p.145, "en realidad lo que implica es que el legislador ha considerado potencialmente peligrosos para estos bienes, especialmente para la intimidad, el acceso informático ilícito. Esto podría expresarse de otra forma si, al igual que ocurre con otros delitos del Código penal, citamos como objeto de protección no el bien jurídico individual que se pretende tutelar, sino el ámbito de seguridad en el que efectivamente se realiza la anticipación de la protección de tales bienes. En este caso hablamos de la seguridad informática […]"

de información y lo hace desde el momento en el que se produce el acceso, sin anticipación alguna. Porque aún en el caso de entender este tipo penal como una medida anticipada, no lo es sólo sobre la intimidad, sino ante cualquier consecuencia que se pueda producir al haberse accedido a un sistema informático ajeno y protegido, consecuencias que pueden ir mucho más allá, y ser mucho más graves, que la mera vulneración de secretos o de la intimidad.

Amén de lo anterior, la vinculación entre el bien jurídico relativo a la seguridad en los sistemas de información y la redacción del acceso ilícito propuesto, permiten una visión completa del tipo penal de forma autónoma junto con el resto de los tipos penales del nuevo Título, además de favorecer las posibles situaciones concursales eventuales con delitos de cualquier otra ubicación en el Código que protejan cualquier otro tipo de interés.

Cabe señalar que, a diferencia de los siguientes delitos, en el acceso ilícito no es requisito del tipo que los datos o programas informáticos sean ajenos a aquel que comete el acceso. Esta situación no es nueva, pues ya se viene dando en la actual legislación. Incardinar este tipo penal en los delitos contra la intimidad puede plantear el problema de si existe tipicidad cuando los datos a los que se accede en el sistema informático invadido son propios (por ejemplo, datos de tráfico o universitarios del que accede), ya que, aunque el tipo penal actual del artículo 197.3 CP no exige la ajenidad, parece difícil que el bien jurídico protegido "intimidad" se vea vulnerado en caso de acceder a datos propios en un sistema informático ajeno. Por ello, aunque la redacción del tipo penal se mantiene en este aspecto, al excluir como bien jurídico principal la intimidad, y señalar como tal la seguridad en los sistemas de información, se viene a producir una justificación reforzada para la existencia de dicho delito, que no castiga tanto la vulneración de la intimidad, que podría no producirse, como ahora sí, y directamente, el atentado contra la seguridad de un sistema de información[773]. Por último, en relación con el artículo 256 CP, la

[773] MORÓN LERMA, E.: *Internet y Derecho Penal: Hacking y otras Conductas Ilícitas en la Red*, Ed. Aranzadi, 2ª edición, Navarra, 2002, p. 67, donde plantea la inadecuación del todavía no tipificado delito de acceso ilícito como delito contra la intimidad; y p. 73, donde expone la idea de la peligrosidad de un acceso ilícito, más allá de que el resultado concreto causado tenga un escasa incidencia en el patrimonio o en la intimidad.

introducción de la acción utilizar, parece colmar el desvalor de éste tipo penal, suprimiendo además el límite de 400 euros, pero añadiendo el elemento referido a que el sistema de telecomunicación (que ahora es sistema informático) tenga que ser utilizado vulnerando las medidas de seguridad. En este caso, y aunque el tipo penal también desaparezca de la sede de delitos patrimoniales, nada impide dicho cambio, pues el aspecto patrimonial clave, que será el perjuicio para el titular del sistema utilizado, podrá ser igualmente resarcido en la responsabilidad civil.

En cuanto a la penalidad establecida, parece adecuado reducir su límite máximo hasta un año y seis meses de prisión. Ello se debe a que, si bien por un lado en la normativa europea no existe mandato específico sobre la misma (aunque una eventual entrada en vigor de la propuesta de Directiva sobre ataques contra los sistemas de información, al establecer un límite superior de al menos dos años provocaría la necesidad de reformar dicho límite), tiene además sentido, que la acción *a priori* menos grave de las que conforman los delitos contra la seguridad en los sistemas de información, tenga la penalidad más reducida. Siendo poco proporcionado que el mero acceso a datos o sistemas informáticos ajenos suponga una acción con el mismo reproche penal que el daño sobre esos mismos objetos.

a.2. Daño informático.

El tipo penal quedaría redactado de la siguiente manera,

> *El que por cualquier medio y sin consentimiento borrase, dañase, deteriorase, alterase, suprimiese, o hiciese inaccesibles datos, programas informáticos o documentos electrónicos ajenos, cuando el resultado producido fuera grave, será castigado con la pena de prisión de seis meses a dos años.*

Se proponen algunos cambios menores y otros más importantes. En primer lugar se sustituye, al igual que en el tipo penal anterior, la expresión "autorización" por la palabra "consentimiento", que en nuestro Derecho es la más adecuada[774].

[774] A ello ya nos referimos en el capítulo tercero de esta investigación al tratar el elemento referido a la "falta de autorización" del actual artículo 264.1 CP.

También se elimina el problema de la doble gravedad de la acción -gravedad en el medio y gravedad en el resultado-. Como ya se ha analizado en esta investigación, la doble gravedad exigida por el tipo es confusa, indeterminada, y hasta cierto punto contradictoria en sí misma, ya que el tipo señala que el medio puede ser cualquiera.

Además, es nuestra opinión, y ya se ha manifestado al analizar las acciones típicas del actual artículo 264.1 CP, que el listado de acciones típicas bien podría reducirse y sustituirse la expresión "borrar, dañar, deteriorar, alterar, suprimir y hacer inaccesible", por las acciones de "suprimir, alterar, o hacer inaccesible"[775], e incluso si de una descripción más general tratásemos con el objetivo de no dejar excluidas otros formas de cometer los atentados contra los datos, programas informáticos o documentos electrónicos en el futuro, limitar el tipo penal a la acción de "dañar"[776]. Sin embargo, ante el mandato europeo, que señala exactamente las mismas acciones que actualmente recoge nuestra regulación penal, parece adecuado, por mor de la estricta transposición, mantener las acciones que el ordenamiento internacional ha señalado[777].

---

[775] El tipo quedaría entonces redactado de esta forma: "*El que por cualquier medio y sin consentimiento suprimiese, alterase o hiciese inaccesibles datos, programas informáticos o documentos electrónicos ajenos, cuando el resultado producido fuera grave, será castigado con la pena de prisión de seis meses a dos años*", aportando, en nuestra opinión una mayor simplicidad tanto para los operadores jurídicos como para el ciudadano que quiere conocer la ley penal, sin haber quedado excluida, en la realidad práctica, ninguna conducta anteriormente tipificada, pues aquellas se pueden reconducir a alguna de las tres acciones resultantes. De forma parecida, aunque sobre la anterior regulación, se manifestaba GONZÁLEZ RUS, J. J.: "Protección…" ob. cit. (sin numerar), al concluir que "centrando la cuestión en los elementos lógicos, penalmente hablando, dañar es equivalente a destruir, deteriorar, inutilizar o alterar una cosa. Por lo menos así los concibe expresamente el art. 264.2 con una formulación tan amplia que hace que tales modalidades de conducta aparezcan como formas de dañar los datos, programas o documentos electrónicos, aceptando implícitamente la posibilidad de que pueda haber otros."

[776] El tipo quedaría redactado como: "*El que por cualquier medio y sin consentimiento dañase datos, programas informáticos o documentos electrónicos ajenos, cuando el resultado producido fuera grave, será castigado con la pena de prisión de seis meses a dos años*". De tal forma, que el daño suponga cualquier acción que modifique los datos, programas informáticos o documentos electrónicos, siempre que se den el resto de requisitos del tipo.

[777] Situación bien diferente a lo que ocurre en el delito de estafa informática del actual artículo 248.2 CP, que sigue igualmente el mandato internacional (Decisión Marco 2001/413/JAI del Consejo, de 28 de mayo de 2001, sobre la lucha contra el fraude y la falsificación de medios de pago distintos del efectivo), y señala como modo de llevar a cabo la acción típica el "valerse de una manipulación informática, o artificio semejante", cuando la Decisión Marco establece, de una forma similar a los daños, que el modo debe ser "la introducción, alteración, borrado o supresión indebidos de datos

Tanto el objeto material del delito, como la necesidad de la producción del resultado grave para la consumación del tipo mantienen la redacción actual. Sin embargo, sobre el significado de "resultado grave" caben ciertas matizaciones de importancia en nuestro estudio, que dependerán fundamentalmente de la ubicación del tipo penal en el Código. Así, una vez excluido este tipo penal de los delitos patrimoniales y de daños, podemos desprendernos de la problemática surgida por la cuantificación económica del daño patrimonial clásico y establecer una nueva interpretación del resultado, en la que la cuantificación económica aparezca, pero con unas características generales sustancialmente diferentes. Al ubicar este tipo penal entre las acciones que vulneran el bien jurídico de la seguridad en los sistemas de información debemos construir ahora la vinculación entre tal vulneración de dicho bien jurídico con la expresión del resultado grave. Es decir, debemos determinar cuándo el resultado es grave desde el punto de vista del bien jurídico protegido, que como hemos señalado, no es -aunque puede ser un factor de determinación- el valor patrimonial concreto de los datos, programas informáticos o documentos electrónicos. Por lo tanto para establecer dicha relación se deben señalar, al menos de forma orientadora, qué resultados deben ser considerados graves desde el punto de vista de la vulneración de la seguridad en los sistemas de información.

Al ser el bien jurídico digno de protección la seguridad en los sistemas de información, la aparición de una situación de desconfianza hacia la utilización de los mismos será la primera consecuencia lógica de la vulneración de dicho bien, por cuanto la sociedad deja de considerar a los sistemas de información como elementos seguros para conseguir un auto desenvolvimiento completo de su personalidad[778]. Así, las situaciones que generan desconfianza pueden ser consideradas todas aquellas en las que se ha producido la pérdida de datos, programas informáticos o documentos electrónicos, para cuya consecución se ha empleado una cantidad de tiempo

---

informáticos, especialmente datos de identidad, o la interferencia indebida en el funcionamiento de un programa o sistema informático". De esta forma, el legislador español reduce considerablemente el listado (de una forma similar a la propuesta para los delitos de daños y sabotaje), sin que parezca que se produzca una deficiencia en la tipificación de la conducta. Sobre este punto véase FARALDO CABANA, P.: "Los conceptos…" ob. cit. pp. 41 y 42.

[778] Se debe reconocer, en todo caso, que éste no será sino el principio general desde el que partir, pues es un factor demasiado abstracto para medir de forma concreta la gravedad de las acciones típicas que eventualmente se puedan cometer.

razonable, y cuya seguridad y guarda se le ha confiado al sistema informático. Como se puede observar, tal forma de apreciar la gravedad del hecho deja en manos de los Tribunales de justicia amplias posibilidades de interpretación que en la actualidad, al menos en teoría, se encuentra restringida con la vinculación de la gravedad exclusivamente al valor económico directo y concreto. La consecuencia de la alternativa que se propone permite que acciones que con la actual regulación pudieran ser atípicas y sobre las que ya nos hemos detenido en esta investigación, no puedan quedar impunes o, en el mejor de los casos, resarcidas en la vía civil, cuando de su naturaleza y consecuencias pocas diferencias podemos encontrar con aquellas que sí encuentran cobijo en la actual regulación penal[779]. No obstante, si bien el perjuicio patrimonial directo debe seguir siendo considerado uno de los factores para determinar la gravedad del resultado, no es el único. Así, estos factores serían los siguientes:

1.- El perjuicio patrimonial directo. Ya hemos señalado que al incardinar este tipo penal bajo la rúbrica de los delitos de daños, la apreciación de la gravedad del resultado debía considerarse en función del valor económico de lo dañado, que no siempre es sencillo de cuantificar cuando hablamos de objetos inmateriales y que además se veía condicionado por diferentes motivos en el ámbito informático. Sin embargo, ello no supone impedimento para que éste sea uno de los puntos esenciales que debe guiar al tribunal a la hora de determinar la gravedad del resultado producido y la determinación de la pena.

2.- El perjuicio patrimonial indirecto: el coste de recuperación. A diferencia de los delitos patrimoniales de daños, donde se situaban anteriormente estas figuras, un factor importante para la apreciación de este nuevo tipo de daño informático son factores de contenido patrimonial que encuentran una vinculación indirecta con la acción típica. Fundamentalmente es el referido al coste de recuperación de los datos, programas informáticos o documentos electrónicos, o incluso del sistema informático

[779] Podemos ahora recordar los problemas que se plantean cuando los datos, programas informáticos o documentos electrónicos son recuperables por la vía del *backup*, o cuando nos encontramos ante objetos de dudoso valor patrimonial como fotografías o música, elementos claramente afectados por la comisión de este tipo de acciones, pero que encuentran una difícil cabida en el concepto de resultado grave desde el punto de vista del perjuicio económico directo, habitual en los delitos de daños.

en su conjunto. Si bien con la regulación actual estos costes no pueden ser tenidos en cuenta a la hora de determinar el valor patrimonial del daño, con el marco legislativo propuesto, no sólo serían un factor de determinación de la gravedad del hecho, sino que en muchos casos resultarían el factor fundamental.

3.- La imposibilidad de la utilización temporal o definitiva. En estrecha relación con la cuestión anterior, recordamos que la interpretación clásica de los daños patrimoniales se construye sobre la idea de que el objeto que ha sufrido el daño ha quedado inutilizado o destruido de forma permanente. Como ya se ha apuntado, es complicado que este hecho se produzca en el ámbito informático al haber, al menos en un número amplio de casos, la existencia de copias de seguridad o *backups* que permiten que, en realidad, no se consiga el resultado a pesar de que el sujeto activo haya desplegado todas las acciones necesarias para conseguirlo. Esta situación genera dudas en cuanto a la consumación efectiva del delito, o si, en cambio, siempre que exista una copia de respaldo de los datos o programas informáticos, o de los documentos electrónicos, estaremos ante una tentativa y no un delito consumado. Por ello, considerar el tiempo en que los sistemas quedan inutilizados, o el tiempo necesario para restaurar los programas informáticos o los documentos electrónicos, como factores para determinar la gravedad de los hechos, parece razonable, especialmente a efectos de considerar consumado el delito, evitando las dudas que se suscitan haciéndolo acorde a la doctrina clásica de los delitos de daños.

4.- La aparición de una situación de desconfianza hacía el ofendido. Determinar si el resultado de la acción ha sido grave encuentra otra forma de cuantificación en los efectos sociales que el ataque pueda producir sobre la persona del ofendido. Esto es, si el ofendido es una compañía que se dedica a las telecomunicaciones[780] posiblemente el daño no produzca una pérdida definitiva de datos, programas informáticos o documentos electrónicos, y además su recuperación sea cuestión de horas (o minutos) debido a los potentes sistemas de copia de seguridad. Sin embargo, todos somos conscientes hoy en día de lo que supone un ataque a una compañía y la trascendencia pública que adquieren estos hechos, de tal forma que una vulneración

[780] Por ejemplo el ataque sobre una compañía que aloja los servidores con los clientes que dan acceso a una tercera empresa de venta por Internet.

grave de la seguridad de ésta, aunque patrimonialmente tenga efectos mínimos, genera un efecto negativo en torno al perjudicado que trasciende del mero perjuicio patrimonial directo o indirecto. Entronca esta forma de medir la gravedad del resultado directamente con la capacidad de generar una situación de desconfianza hacia los sistemas de información en la sociedad que, como hemos señalado, es realmente la forma primaria de entender vulnerado el bien jurídico protegido.

De la enumeración anterior podemos extraer una conclusión básica, y es la transformación de elementos de apreciación y cuantificación en la jurisdicción civil como factores de medida de la gravedad del resultado producido por los hechos en la jurisdicción penal, de tal forma que de alguna manera lo que se está admitiendo es una forma de cuantificar la gravedad del resultado en función de un perjuicio patrimonial en sentido amplio, de forma opuesta a cómo el Derecho penal de daños ha venido interpretando dicho perjuicio patrimonial a la hora de interpretar los tipos penales del artículo 263 CP y otros análogos[781]. Tal forma de interpretar la gravedad radica en la realidad inmaterial ante la que nos encontramos, totalmente diferente a la de los objetos que el legislador y el operador del Derecho clásicos pudieron tener en cuanto a los daños sobre objetos materiales físicos. El concepto de daño o el de desaparición de la cosa son aplicables difícilmente en cuanto a los datos, los programas informáticos o los documentos electrónicos precisamente por su naturaleza inmaterial. En este ámbito, la destrucción o inutilidad definitiva de los objetos materiales es por su propia naturaleza posible, pero mucho menos probable, y a esta diferente naturaleza debe dar una respuesta adecuada el legislador actual que encuentra dificultades obvias con la ubicación y tipo de delitos entre los cuales se han considerado los daños informáticos en el vigente Código penal. Por ello, en los atentados contra los sistemas informáticos o sus componentes lógicos (datos informáticos en general, documentos electrónicos o programas informáticos), lo relevante no sólo es la destrucción definitiva de los mismos, sino los efectos que esto

[781] CAMACHO LOSA, L.: *El delito…* ob. cit. pp. 29 y 30, comentaba ya en 1987 respecto del perjuicio patrimonial en el fraude informático que éste iba más allá del perjuicio patrimonial directo, sumándose el perjuicio indirecto, y el perjuicio intangible, relacionándolos con el lucro cesante el primero y el daño a la imagen, el honor o la estima pública en el segundo. Siendo en muchos casos el objetivo primario del atacante el de conseguir uno de estos dos perjuicios, y no necesariamente un impacto patrimonial directo en la víctima.

produce y la complicación (por motivos económicos y de tiempo principalmente) de restaurar los sistemas o sus datos a su estado original, pues si bien es muy probable que esto finalmente se produzca, el daño debe considerarse realizado y valorado como grave. Además, esta extensión interpretativa respecto de los daños clásicos y los actuales daños informáticos da respuesta a los problemas que se suscitan principalmente en torno a la naturaleza de los documentos electrónicos atacados cuando estos tienen un carácter personal, de difícil estimación económica y que con la actual regulación generan dudas respecto de si las acciones típicas sobre estos objetos no completan el tipo penal, interpretación a nuestro juicio discutible, ya que del mandato europeo no se extraen especiales excepciones respecto de qué datos, programas informáticos y documentos electrónicos deben ser dignos de protección penal, y cuáles no; entendiendo que la protección es general para todos ellos, independientemente de su naturaleza, siempre que sea informática. Esta nueva interpretación se ajusta además convenientemente al bien jurídico tutelado propuesto para estos delitos, que no es tanto el patrimonio -que también- como la seguridad en los sistemas informáticos, que se ve vulnerada en el momento que se ataca un sistema informático o sus elementos, independientemente de cual sea el contenido de éstos, ya sea la base de datos de una compañía, unas fotografías o el borrador de una tesis doctoral.

Debemos señalar, en todo caso, que la lista que hemos propuesto para el cálculo de la gravedad del resultado no es cerrada, y podrían pertenecer a ella otros supuestos que serán objeto de la práctica jurisprudencial y el estudio doctrinal. Si bien, y en todo caso, aunque es verdad que su apreciación puede resultar inexacta, el valor fundamental que se debe proteger al tipificar estos delitos es la confianza en la utilización de sistemas informáticos por parte de los ciudadanos, por lo que en todo caso, al margen del valor económico directo o indirecto de los objetos materiales dañados o los problemas derivados de dichos daños, la gravedad se debe medir, conforme al principio de intervención mínima del Derecho penal, con base en la capacidad de generar desconfianza en la utilización de sistemas de información como consecuencia de los hechos presuntamente delictivos ocurridos, pudiendo actuar como baremo para medir dicha desconfianza el resto de posibilidades de la lista, u otras que puedan aparecer en el futuro.

Por último, en cuanto a la penalidad propuesta, ya se ha señalado en esta investigación, con las dudas pertinentes, que el legislador ha decidido establecer el límite superior de dos años para tal acción, siendo un término intermedio entre el año mínimo exigido y los tres años permitidos, de tal forma que entendemos que tal extremo debe mantener su actual configuración, si bien cabe recordar que la penalidad prevista en la presumible Directiva que sustituya a la Decisión Marco actual establece un límite superior mínimo de dos años, por lo que si bien dicho límite seguiría estando dentro de los marcos exigidos por el ordenamiento europeo, supondría estar en el punto más bajo de la penalidad permitida. En todo caso, puede abrirse el debate sobre si es conveniente que este tipo de acciones delictivas, en principio más graves que las del mero acceso ilícito, compartan la misma penalidad, y si no sería, al menos en cuanto al límite superior, razonable, aumentar el marco penal abstracto entre los seis meses y los 3 años.

a.3. Sabotaje informático.

El tipo penal quedaría redactado de la siguiente manera,

> *El que sin consentimiento obstaculizara o interrumpiera el funcionamiento de un sistema informático ajeno introduciendo, transmitiendo, dañando, borrando, deteriorando, alterando, suprimiendo o haciendo inaccesibles datos informáticos, cuando el resultado producido fuera grave, será castigado, con la pena de prisión de seis meses a tres años.*

Se realizan algunas modificaciones en un sentido similar al tipo penal anterior, se sustituye la expresión autorización, por la de consentimiento y se elimina la doble gravedad ya analizada y debatida en esta investigación.

También se pueden apreciar algunos cambios en el enunciado del tipo penal para ajustar la propuesta al análisis que hicimos del mismo en el capítulo tercero de esta investigación, en el sentido de que las acciones típicas son interrumpir y obstaculizar, y el modo de hacerlo, a diferencia de lo que parece señalar el actual 264.2 CP, no es cualquiera, sino las acciones típicas del delito anterior (borrar, dañar, deteriorar, alterar, suprimir o hacer inaccesibles) junto con la de introducir y

transmitir datos informáticos. Por ello, siguiendo con el espíritu de la actual regulación, se elimina la expresión "cualquier medio", y se dejan exclusivamente los medios realmente hábiles para cometer las acciones típicas; formulación que no excluye que tales modos de realizar alguna de las acciones típicas sean cometidos por cualquier medio, y que simplifica el enunciado del texto penal. Además, sobre el catálogo de modos de llevar a cabo la acción típica puede realizarse el mismo análisis que ya hicimos para el delito de daño informático, en el que creemos que el listado de acciones no tendría por qué ser tan extenso. Se puede asimismo plantear el sustituir los modos coincidentes con el delito anterior al realizar las acciones típicas con una remisión al delito de daño informático, de tal forma que los modos de cometer las acciones de obstaculizar o interrumpir pudiesen ser "introduciendo, transmitiendo o realizando alguna de las acciones del artículo anterior"; tal opción ha sido la utilizada por el legislador en otros países de nuestro entorno, por ejemplo en el ordenamiento penal alemán o italiano[782]. Tratándose en todo caso de una modificación menor, parece preferible respetar la redacción del artículo de la forma más parecida a la opción que el legislador de 2010 decidió otorgar al actual 264.2 CP.

Para la calificación de los hechos como graves se deberá así mismo atender a las premisas expuestas para el daño informático, de tal forma que lo más importante es señalar que el perjuicio patrimonial directo no debe ser considerado como el único factor a tener en cuenta para determinar la gravedad del resultado, como se ha venido haciendo hasta ahora. En efecto, en la misma línea ya explicada para el daño informático, el resultado deberá ser considerado como grave cuando la entidad de la vulneración de la seguridad en el sistema de información afecte de forma severa a la confianza en la utilización de sistemas informáticos, para lo cual será necesario atender, además de a factores económicos, a otros posibles ya señalados.

[782] El §303b StGB, señala como modos de realizar la acción típica de "perturbar considerablemente el procesamiento de datos" (equivalente a nuestro sabotaje informático) las acciones del §303a StGB que regula la modificación ilegítima de datos que equivale, con algunos matices, a nuestro daño informático. Igualmente en el artículo 635 quarter del Código penal italiano señala que los modos de obstaculizar o interrumpir el funcionamiento de un sistema informático podrán ser los contemplados en su artículo 635 bis, equivalente a nuestro delito de daño informático.

Por último, en cuanto a la penalidad, se mantiene la que actualmente recoge el Código penal en su artículo 264.2, y que encuentra acomodo tanto en el mandato internacional proveniente del Convenio sobre la Ciberdelincuencia de Budapest de 2001, como de la Decisión Marco 2005/222/JAI del Consejo, así como en el proyecto de Directiva que viene a sustituir a la Decisión Marco vigente. En todo caso, al igual que señalamos en el tipo penal anterior, cabría la posibilidad de preguntarse, de cara a un futuro, si un hipotético aumento de la penalidad del tipo de daño informático, debería conllevar así mismo un aumento de penalidad, al menos en su límite superior, de la penalidad del sabotaje informático en vista de que las acciones señaladas en este tipo son de mayor gravedad que las de los anteriores. Es importante señalar, aun así, que un aumento de la penalidad por encima de los tres años, no sería acorde con el actual mandato europeo que establece un máximo para el límite superior de tres años, si bien sí sería compatible con el presumible marco penal abstracto que establecerá la Directiva que sustituya a la Decisión, que marca un límite superior de al menos dos años, sin marcar un máximo.

a.4. Abuso de dispositivos.

El tipo penal y la concurrencia con otros tipos de este Título quedarían redactados de la siguiente manera,

> *1. El que produzca, venda, adquiera para el uso, importe, distribuya o realice cualquier otra forma de puesta a disposición de un programa informático, un código de acceso o datos similares concebidos o adaptados con la intención principal de cometer uno de los delitos de este título será castigado con la pena de prisión de seis meses a dos años.*
>
> *2. Cuando con los actos sancionados en el párrafo anterior se ocasionare, además, un resultado lesivo constitutivo de otro delito de este Título, cualquiera que sea su gravedad, los Jueces o Tribunales apreciarán tan sólo la infracción más gravemente penada, aplicando la pena en su mitad superior.*

La tipificación de esta conducta responde, en primer lugar, a las imposiciones del Convenio sobre la Ciberdelincuencia de 2001, y a la más que probable imposición que realice la futura Directiva europea relativa a los ataques contra los sistemas de información. Pero además de suponer la transposición completa de la normativa internacional viene a llenar un vacío grave que se produce en nuestra regulación penal actual, al ubicar los delitos de daños informáticos junto con los daños patrimoniales, pues al seguirse la forma habitual de regular éstos como delitos de resultado, quedan exentas del reproche penal la creación y distribución de virus informáticos y otro software malicioso. En efecto, parecería más complicado, en los delitos de daños clásicos, introducir un tipo penal para cuya consumación sólo fuera necesaria la puesta en peligro del bien jurídico. La distribución de virus informáticos, con la actual regulación, sólo queda contenida de forma muy diluida dentro del delito de daño informático en forma de tentativa o llegado el caso, como una suerte de complicidad o cooperación necesaria; y el tráfico de claves de acceso o contraseñas, aunque de una gravedad objetiva menor[783], tampoco encuentra una respuesta penal adecuada.

Quedaría así configurado el tipo penal como un delito de peligro[784]. El mero hecho de la creación, y todavía en mayor medida con la distribución, resultarían acciones de riesgo de especial entidad para el bien jurídico protegido. Esta cuestión ya ha sido señalada por la doctrina[785].

---

[783] La puesta en peligro del bien jurídico protegido (seguridad en los sistemas de información) resultará de menor entidad en el caso del tráfico de claves de acceso, que en todo caso permitirán cometer directamente el delito de acceso ilícito pero nunca, de forma directa, implicarán los de daños y sabotaje, sino que necesitarán de algo más por parte del actor. En cambio, el tráfico de virus informáticos y programas análogos sí puede generar una mayor puesta en peligro del bien jurídico al no tener por qué necesitarse, en principio, más acciones que el mero envío de los mismos para producir los daños. En todo caso, el tipo penal propuesto, como veremos a continuación, encuentra un marco penal abstracto suficientemente amplio como para poder dejar en manos de los Tribunales la valoración del riesgo real en cada caso.

[784] QUINTERO OLIVARES G.: *Parte*… ob. cit. pp. 348 y ss. o MIR PUIG, S.: *Derecho*... ob. cit. pp. 229 y ss.

[785] MAZA MARTÍN, J. M.: "La necesaria…" ob. cit. p. 300, sugiere la idea "de adelantar las barreras de protección penal, con la incorporación de la figura del delito de riesgo informático para todas aquellas conductas que supongan un concreto peligro para los sistemas o redes informáticos, sin que la consumación de ese propósito hubiese llegado efectivamente a alcanzarse". También ROMEO CASABONA, C. M: "De los delitos…" ob. cit. p. 16.

Se debe señalar que estás acciones no se encuentran tipificadas en todos los países de nuestro entorno. En el Código penal italiano no podemos encontrar un tipo penal parecido a este. En el StGB se tipifican los actos preparatorios para cometer los delitos de acceso ilícito, daños, y sabotaje. Sin embargo tal hecho parece responder más a la propia estructura del Código penal que a una verdadera trasposición de la normativa internacional, que como hemos visto en esta investigación, va a más allá de exigir la tipificación de los actos preparatorios y construye verdaderos tipos penales de peligro con una serie de elementos detallados. Por el contrario el Código penal francés sí regula como tal el abuso de dispositivos en el artículo 323-3-1, y remite a los delitos de acceso, daño y sabotaje informático para establecer las penas a aplicar. En la regulación penal británica, la última reforma de la *Computer Misuse Act* de 1990 llevada a cabo en el año 2007 introducía en la sección tercera el subapartado A tales acciones, con una penalidad de hasta 1 año de prisión (misma penalidad con la que castiga el acceso ilícito, el daño y el sabotaje informático). En todo caso es adecuado decir que la introducción de este tipo penal, de la forma en que estime oportuno cada Estado, será una cuestión de los legisladores de los distintos países, si bien con ella se deberá dar cumplimiento a la normativa internacional.

Por lo respecta a la penalidad elegida, se ha entendido que la gravedad para las acciones de daños informáticos y figuras conexas que ha impuesto el legislador español, siguiendo el mandato internacional, aconseja que la penalidad de las acciones de abuso de dispositivos mantengan una proporcionalidad con las figuras principales (así se observa en el caso de Francia o Reino Unido). De ahí que la pena elegida sea análoga a la pena media prevista para los tipos penales principales, partiendo del año y seis meses máximo de prisión para el acceso ilícito, y de los tres años para el sabotaje informático, nos hemos decantado por una penalidad máxima de dos años prisión. En todo caso y como ya hemos manifestado, la presumible entrada en vigor de la Directiva relativa a los ataques contra los sistemas de información en próximas fechas puede generar la necesidad de revisar este extremo en un futuro próximo.

Por último, en este mismo artículo se contempla, de forma similar a otros preceptos del Código, la solución al problema concursal que pueda aparecer cuando este tipo penal concurra con alguno de los anteriores, especialmente pensando en la situación en que un sujeto adquiera un programa malicioso o una clave para ejecutar a continuación un delito contra la seguridad en los sistemas de información (acceso, daño o sabotaje informático) resolviendo de tal forma que sólo se aplique la pena del tipo penal más grave en su mitad superior.

B) SUPUESTOS AGRAVADOS EN LOS DELITOS CONTRA LA SEGURIDAD EN LOS SISTEMAS DE INFORMACIÓN

Una de las cuestiones que deben revisarse es la relativa a los tipos agravados de los delitos anteriores, en los que se pueden reunir ciertos aspectos dispares. Por un lado no se debe renunciar a los supuestos agravados ya contemplados en nuestra legislación penal, independientemente de que en la actualidad los delitos que conformarían este nuevo Título se encuentren dispersos en el Código. En segundo lugar se deben atender los mandatos internacionales que imponen determinadas pautas en la regulación y en tercer lugar no se debe renunciar, independientemente de los extremos ya regulados y aquellos exigidos por la normativa internacional, a completar de la mejor forma posible la actual regulación con supuestos agravados que puedan suponer una especial puesta en peligro del bien jurídico protegido. De esta manera, el texto del artículo referido a los supuestos agravados quedaría redactado de la siguiente manera,

> *Se impondrán las penas superiores en grado a las respectivamente señaladas en los artículos anteriores y, en todo caso, la pena de multa del tanto al décuplo del perjuicio ocasionado, cuando en las conductas descritas concurra alguna de las siguientes circunstancias:*
> *a) Se hubiesen cometido en el marco de una organización criminal.*
> *b) Se hayan podido derivar consecuencias de especial gravedad. Se entenderá que pueden derivar consecuencias de especial gravedad en todo caso cuando:*
> *1. Hayan podido afectar a los intereses generales.*
> *2. Hayan podido afectar a una pluralidad de personas.*

3. Se cometan contra el sistema de información de una infraestructura crítica

Con la proposición que venimos realizando se cumple uno de los requisitos establecidos en los marcos internacionales, y es que las tres acciones principales de acceso, daño y sabotaje cuenten con un serie de supuestos agravados comunes, realidad que no se viene produciendo en la actualidad, al encontrarse el supuesto de acceso ilícito en el artículo 197.3 CP, y no contemplarse para el mismo los supuestos agravados del actual 264.3 CP que sólo afectan a daño y sabotaje informático. Por lo demás, en principio, se mantienen los supuestos ya tipificados en el artículo 264.3 CP relativos a la realización de los tipos penales en el ámbito de una organización criminal y cuando el resultado revista una especial gravedad, cuestión sobre la que podemos matizar, al igual que en los supuestos básicos, que no deberá ser tenida en cuenta tan sólo desde el punto de vista puramente económico. En realidad, estas dos agravantes son las que ya se establecen en la actual Decisión Marco 2005/222/JAI del Consejo, y no es sino en su detalle en lo que se ha trabajado en la propuesta de Directiva que todavía no ha sido aprobada.

Así, la agravación debida a los intereses generales ocupa un nuevo subapartado y se engloba, por su conexión, junto con la afectación a una pluralidad de personas, ambas junto al supuesto en el que alguno de los delitos contra la seguridad en los sistemas de información se cometa sobre sistemas informáticos que pertenezcan a infraestructuras críticas. Todos estos supuestos en realidad son casos concretos de la agravación genérica relativa a la especial gravedad. Parece correcto, desde un punto de vista de técnica legislativa, enumerar tan sólo dos supuestos agravados que realmente tienen una naturaleza diferente (que la acción delictiva se cometa en el contexto de una organización criminal es un motivo muy diferente a que de las acciones se puedan derivar consecuencias de especial gravedad) y englobar dentro de las segundas un listado abierto de todas las posibles situaciones en las que se puede producir tales efectos. Las tres opciones propuestas se encuentran en la actual propuesta de Directiva y se refieren a los intereses esenciales (esta también recogida en la vigente Decisión Marco), cuya naturaleza ya ha sido discutida en esta investigación, que afecte a una pluralidad de personas, introducida en la

actual propuesta de Directiva o finalmente que se cometan contra los sistemas de información de una infraestructura crítica, sobre las que ya nos detuvimos en esta investigación en el capítulo segundo[786].

En todo caso se debe señalar que, del texto propuesto, no se debe extraer que los únicos casos de especial gravedad sean los contemplados en los tres subapartados, sino que se señala únicamente que los casos recogidos serán siempre de especial gravedad, de acuerdo con el proyecto de la actual Directiva relativa a los ataques a los sistemas de información, quedando en manos de los Tribunales determinar -y de la doctrina proponer- a partir de qué otros supuestos se pueden derivar igualmente consecuencias de especial gravedad.

Por último, la penalidad establecida, al señalar que se aplicarán las penas superiores en grado, permite que se cumplan los marcos exigidos por la regulación europea, que establece que el límite superior cuando se de alguna de estas circunstancias sea de entre dos y cinco años para los delitos de acceso ilícito, daño informático y sabotaje informático[787]. Si bien, al igual que hemos venido señalando, la aprobación del proyecto de Directiva que sustituya la Decisión Marco actual va a requerir una revisión de tales marcos penales, al exigir un límite superior mínimo de 5 años para dichos tipos agravados, límite que no se cumple en ninguno de los tipos con la actual regulación.

En cuanto a otras agravantes contempladas en el Código que afectan actualmente a los artículos 197.3, 264.1 y 264.2 CP debemos hacer referencia a lo siguiente: en cuanto a las que afectan al acceso ilícito (artículos 197.4, 197.6 y 197.7 CP), podemos señalar que al menos el caso del artículo 197.4 CP parece requerir, por la propia naturaleza del tipo, el apoderamiento de los datos, lo que no ocurre en el ámbito del artículo 197.3 CP (sí, en cambio, en los apartados primero y segundo). El

[786] Sobre la importancia de dicha agravante véase el trabajo de COHEN, F.: "Cyber-risks and critical infrastructures" en *Strategic Security*, vol. 27, nº 2, 2003, pp. 1-10, en el que se llega a recoger cómo bienes jurídicos totalmente esenciales como la vida humana se puede llegar a poner en riesgo cierto ante este tipo de conductas.

[787] El acceso ilícito agravado tendría una pena de prisión de 1 año y 6 meses a 2 años y 5 meses, el daño informático también de 2 a 3 años de prisión, el sabotaje informático de 3 a 4 años y 6 meses de prisión.

apartado sexto exige que se imponga la pena en su mitad superior cuando se "afecten a datos de carácter personal que revelen la ideología, religión, creencias, salud, origen racial o vida sexual, o la víctima fuere un menor de edad o un incapaz" de tal manera que la hipotética desaparición del supuesto agravado siempre podrá ser suplida con la interpretación jurisprudencial a través de la agravante de especial gravedad. El apartado séptimo[788] puede ser resuelto, en parte, a través de la agravante genérica del artículo 22.3 CP (ejecutar el hecho mediante precio, recompensa o promesa) de tal manera que ésta supla la mención expresa en el tipo penal. Además, el artículo 198 CP establece una agravación en el caso de que el delito lo haya cometido un funcionario o cargo público, que supone, además de la aplicación de la pena en su mitad superior, la inhabilitación absoluta de 6 a 12 años. Aun planteándose la posibilidad de introducir dicha agravante dentro del catálogo propuesto para mantener la configuración lo más parecida a la vigente, existen algunas razones para no hacerlo: por un lado, porque la potestad del juez o tribunal de condenar accesoriamente a la inhabilitación especial para empleo o cargo público (artículo 56.3 CP en relación con el 42 CP) así como apreciar la agravante genérica del artículo 22.7 CP (prevalerse del carácter público que tenga el culpable) puede paliar los efectos del cambio propuesto, y por otro lado, porque de la naturaleza que adquiere el acceso ilícito con la nueva formulación propuesta, derivada de las exigencias internacionales, la intimidad cede en favor de la seguridad en los sistemas de información, de tal forma que los motivos que agravan los tipos básicos giran en torno a la gravedad del ataque sobre los sistemas de información, y no a otras cuestiones como la protección de la intimidad. Además, en la línea de los supuestos agravados del propio artículo 197 CP, la existencia de dicho supuesto responde más correctamente a los apartados primero y segundo, que al tercero, cuya naturaleza y formulación es visiblemente diferente.

Los supuestos agravados que afectan a los actuales 264.1 y 264.2 CP y que no se contemplan al menos directamente en la proposición realizada son los relativos al artículo 266.2 CP sobre el que se pueden realizar algunas precisiones: en primer

[788] Artículo 197.7 CP: Si los hechos se realizan con fines lucrativos, se impondrán las penas respectivamente previstas en los apartados 1 al 4 de este artículo en su mitad superior. Si además afectan a datos de los mencionados en el apartado anterior, la pena a imponer será la de prisión de cuatro a siete años.

lugar, el hecho de cometer los daños informáticos (que recordemos son daños sobre elementos lógicos y no físicos) "mediante incendio, o provocando explosiones o utilizando cualquier otro medio de similar potencia destructiva, o poniendo en peligro la vida o la integridad de las personas", provoca el concurso del delito de daños clásicos del artículo 263 CP con los daños informáticos del artículo 264 CP (siempre que el daño físico sea medio para cometer el daño informático), en cuyo caso, la agravante ya se aplicará sobre los daños del artículo 263 CP, de tal forma que se deberá resolver el concurso entre los daños del artículo 263 CP agravados por el 266.2 CP con el 264.1 o 264.2 CP y por lo tanto y en todo caso la agravante sería considerada. Pero dejando al margen este razonamiento, en segundo lugar, podemos acudir a un problema que vas más allá de la propuesta realizada. La configuración de los artículos 263 y 264 CP, con respecto al 266.1 y 266.2 CP responde a un problema de incongruencia legislativa manifestada incluso por los tribunales de justicia[789] a raíz de la entrada en vigor de la LO 5/2010 de 22 junio de reforma del Código penal en la cual el legislador no ha cambiado las referencias del artículo 266 CP a la nueva distribución de los daños que instauraba dicha reforma. Así, el artículo 266.1 CP en realidad debería referirse al 263.1 CP, y el 266.2 CP al 263.2, de tal manera que los daños informáticos, entre otras cosas, por su alta penalidad *per se*, quedarían excluidos de la aplicación de estos supuestos agravados.

[789] SAN 5/2012 de 6 de febrero, F.J. 8º: "dicho lo anterior, partiremos de los daños comunes del art. 263, que, al ser cometidos mediante incendio, hay que poner en relación con el art. 266, reiterando que estamos hablando de esos artículos tal como quedaron tras la reforma operada en el CP por LO 5/2010, por ser más favorable al reo. No descartamos que este efecto favorable al reo sea producto de un descuido del legislador, que ha traído consigo dicha reforma, desde el momento que el art. 266 está contemplando una pena de prisión de uno a tres años para cualquier modalidad de daños del art. 263, ya sean los básicos de su apdo. 1, ya sean los cualificados de su apdo. 2, cuando se causan mediante incendio, pues ello no deja de encerrar una antinomia, si se compara con los daños cualificados del apdo. 2 del art. 263, que, sin ser ocasionados mediante incendio, tienen prevista la misma pena de prisión de uno a tres años y, además, una multa de doce a veinticuatro meses, esto es más grave; como también si se compara con que los daños informáticos, introducidos tras la reforma en el art. 264, que en su modalidad básica llevan aparejada una pena menor (de seis meses a dos años de prisión), sin embargo, si este entra en aplicación en relación con el art. 266, lleva aparejada una pena mayor (de tres a cinco años de prisión y multa de doce a veinticuatro meses), que la que corresponde a los daños materiales cualificados del apdo. 2 del nuevo art. 263, tanto los no ocasionados mediante incendio (de un año a tres de prisión y multa de doce a veinticuatro meses), como los que se ocasionen mediante él (de uno a tres años de prisión, por el juego del art. 266). Desde luego, no parece que, por muy ambiciosa que haya querido ser la reforma, fuera la voluntad del legislador sancionar más gravemente los daños informáticos que los comunes, en todos los casos y sin distinciones."

En todo caso, y para finalizar, los supuestos agravados propuestos permiten suficiente interpretación jurisprudencial, y parecería del todo ilógico que acciones como las previstas en los supuestos agravados tanto del acceso ilícito como de los daños informáticos que con la propuesta dejan de estar contempladas explícitamente, pasasen desapercibidas al juzgador, que podría introducirlos motivadamente a través del supuesto agravado relativo a la especial gravedad, que como ya hemos señalado, no se agotaría con la numeración propuesta.

C) RESPONSABILIDAD PENAL DE LAS PERSONAS JURÍDICAS

El aspecto relativo a la responsabilidad penal de las personas jurídicas varía respecto de la actual regulación en cuanto a la penalidad establecida, quedando redactado de la siguiente manera,

> *Cuando de acuerdo con lo establecido en el artículo 31 bis una persona jurídica sea responsable de los delitos anteriores, se le impondrá la pena de multa de seis meses a tres años para los tipos básicos, y de tres años a 4 años y seis meses para los supuestos agravados. Atendidas las reglas establecidas en el artículo 66 bis, los jueces y tribunales podrán asimismo imponer las penas recogidas en las letras b a g del apartado 7 del artículo 33.*

Se deben señalar dos aspectos de la redacción propuesta: por un lado se ha unificado la penalidad para todas las conductas típicas, a diferencia de cómo se encuentra en la actual redacción en la que para el tipo de acceso ilícito la penalidad determinada es de seis meses a dos años (197.3 párrafo 2º CP), mientras que para el delito de daño y sabotaje informático la penalidad varía entre la pena de multa del doble al cuádruple del perjuicio causado, si el delito cometido por la persona física tiene prevista una pena de prisión de más de dos años y la pena de multa del doble al triple del perjuicio causado, en el resto de los casos (264.4.a y 264.4.b CP). Si bien respecto a la penalidad para el acceso licito apenas sufre un ligero aumento, el cambio sustancial se realiza en cuanto la penalidad entre el actual 264.4 CP y la ahora propuesta, no tanto por la concreción final, para cuyo problema siempre se puede atender a la determinación realizada en los Tribunales, como si a la forma de

cálculo de dicha responsabilidad penal. Mientras que en la actual regulación el marco abstracto se establece en función del perjuicio patrimonial causado (razonable en cuanto a su ubicación sistemática en el Código penal), en la proposición se prefiere determinar un marco abstracto fijo que no dependa del perjuicio causado, principalmente porque la determinación del perjuicio causado, especialmente en el delito de acceso ilícito y de abuso de dispositivos, pero también en otros supuestos de daño y sabotaje, puede ser equivalente a cero, de tal manera que quedaría impune la acción cuando de una persona jurídica se tratase. Podemos pensar en la compañía que vende programas informáticos maliciosos a terceros o que realiza acceso ilícitos a sistemas de seguridad de la competencia con fines diversos (por ejemplo, copiar el sistema de seguridad para implantarlo en su propia empresa); en estos supuestos, el perjuicio patrimonial es dudoso y en todo caso enormemente difícil de calcular, lo que llevaría a una indeterminación poco aconsejable en el texto penal. Por ello, parece aconsejable acudir a un marco abstracto determinado, entre otras cosas porque, por otro lado, se ha establecido un marco penal suficientemente amplio dentro de los márgenes permitidos en el artículo 50.3 CP, y con previsión expresa de la penalidad en caso de darse alguno de los supuestos agravados, que puede colmar la desaparición de la pena proporcional al perjuicio causado que se establece en el actual 264.4 CP.

Por último, tanto el actual 197.3 CP como el 264.4 CP establecen la posibilidad de aplicar las penas recogidas en el artículo 66 bis CP, en concreto aquellas de las letras b a g, por lo que en este extremo la regulación propuesta mantiene la elegida por el legislador de 2010.

D) OTRAS REFORMAS VINCULADAS

Además de las modificaciones propuestas, no se debe pasar por alto que el Código penal no está compuesto por artículos aislados, sino que es un sistema en su conjunto, y como tal debe observarse cualquier modificación en el mismo. Al margen de las necesarias modificaciones en cuanto a la numeración de los artículos, aceptar la propuesta de regulación anterior implica otros cambios en el Código penal en orden a que este mantenga esa cohesión interna que siempre debe mostrar. A este respecto podemos señalar:

1- Supresión del actual 197.3 CP: la figura del acceso ilícito en su actual ubicación debería ser suprimida, conllevando la remuneración de los siguientes apartados del artículo 197 CP.

2.- Supresión del actual 256 CP: ya se ha señalado que al introducir la acción de utilizar un sistema informático ajeno en la proposición del nuevo delito de acceso ilícito, no sería necesario la existencia de dicho precepto.

3.- Supresión del actual 264 CP: se propone la vuelta a la situación previa a la reforma de 2010, en la cual los supuestos agravados de los daños del artículo 263 CP ocupaban este artículo. Ello además corrige un problema de deficiencia legislativa producido a raíz de dicha deforma de 2010, respecto del actual 266.2 CP[790].

4.- Posible tipificación de una falta contra la seguridad en los sistemas de información: no parece adecuado, acorde a los principios de mínima intervención del Derecho penal, así como a los mandatos internacionales, la tipificación de una falta para los supuestos propuestos más leves, quedando para ello la vía civil para reclamar por los posibles daños y perjuicios causados en actuaciones que implican las acciones típicas propuestas, pero cuyo resultado no se pueda computar grave. Además, desde el poder ejecutivo y legislativo se prevé en la actualidad la próxima desaparición del Libro III del Código penal que regula las faltas[791], lo que supone un motivo más para mantener la idea de excluir esta posibilidad.

5.- Posible tipificación de delitos imprudentes: podría plantearse la necesidad de regular un tipo imprudente relativo a la seguridad en los sistemas de información. En la línea manifestada sobre la hipotética falta, la perspectiva de esta proposición se inclina en todo caso por la impunidad de la imprudencia (incluida la grave) en los delitos contra la seguridad en los sistemas de información, debiendo reconducirse en todo caso tal situación a la vía civil.

[790] A ello ya nos referimos al hablar de los supuestos agravados del artículo 266.2 CP respecto del actual 264 CP y la sentencia de la Audiencia Nacional 5/2012 de 6 de febrero.

[791] Disposición derogatoria única del anteproyecto de reforma del Código penal de 2012 que fue aprobado por el Consejo de Ministros celebrado el 11 de octubre de 2012 y se encuentra actualmente en tramitación parlamentaria en las Cortes Generales.

6.- Desaparece la posible aplicación de la excusa absolutoria del artículo 268 CP en los delitos de daños y sabotaje informático: sobre la vigencia de esta figura, se acepte o no la proposición formulada, ya nos manifestamos en el capítulo tercero de la investigación, siendo en todo caso la reforma propuesta una vía posible de suprimir dicha posibilidad en estos delitos.

7.- Modificar los delitos de desórdenes públicos: se busca dar cabida a los delitos informáticos añadiendo un apartado 4, en el artículo 560 CP que establezca que "*los que con el fin de atentar contra la paz pública, alteren el orden público cometiendo alguno de los delitos contra la seguridad en los sistemas de información del Título "x"* (el relativo a los delitos contra la seguridad en los sistemas de información), *serán castigados con la pena de prisión de uno a cinco años, sin perjuicio de las penas que les puedan corresponder conforme a otros preceptos de este Código*". De la misma manera se recomienda suprimir la referencia a la obstaculización de los sistemas de telecomunicaciones del actual artículo 560.1 CP, pues dicha acción quedaría contemplada como una de las acciones contra la seguridad en los sistemas de información del precepto propuesto. La estructura sistemática del Código parece indicar que sea esta la mejor forma de tipificar estas conductas, aun cuando se plantea la posibilidad, especialmente por la similitud en los marcos penales abstractos, de crear un supuesto agravado específico en el Título relativo a los delitos contra la seguridad en los sistemas de información referida precisamente a realizar alguna de las acciones típicas con el fin de alterar el orden público.

CONCLUSIONES DE LA INVESTIGACIÓN

CONCLUSIONES DE LA PRIMERA PARTE

La expansión exponencial de la ciberdelincuencia es innegable y así lo demuestra la dedicación que a estas nuevas prácticas delictivas han dado los diferentes Estados en sus normativas. Estamos ante un fenómeno relativamente novedoso, que además tiene una característica inherente al desarrollo tecnológico; la tecnología avanza a un ritmo vertiginoso, y este tipo de delitos, su aparición y su desarrollo tienen, en contradicción con el lento avance del Derecho, esa misma característica. Prueba de ello son los interesantes informes elaborados por el IC3 norteamericano donde se encuentran tablas cronológicas referidas al aumento de este tipo de delitos, e igualmente a las estadísticas que manejan las empresas privadas en cuyos múltiples informes también se recoge el indudable crecimiento exponencial de estas conductas prohibidas, o la recentísima puesta en funcionamiento del EC3 en la Unión Europea para coordinar la respuesta ante ciberataques en los Estados de la Unión.

Respecto al tratamiento legal otorgado a los daños informáticos por el ordenamiento internacional, cabe destacar el acierto que supone que estas situaciones sean reguladas por un marco general supranacional como punto de partida, estableciendo los mínimos comunes para todos los Estados. La informática tiene un carácter trasnacional obvio. Nunca sería suficientemente protectora una regulación en un Estado, si no existe una regulación afín en el resto de Estados, pues la comisión de estos delitos, siempre que se utilicen medios informáticos para realizarlos, no necesitan de la cercanía física. Pueden producirse desde tan lejos como alcance una red de comunicación que permita el acceso a Internet. Por ello, lo ideal es que todos los Estados (o por lo menos la mayoría) suscriban el Convenio sobre la Ciberdelincuencia celebrado en Budapest en 2001 o, en el seno de la Unión Europea, se realice la trasposición adecuada por parte de todos los Estados miembros de la Decisión Marco 2005/222/JAI del Consejo. Un solo Estado que no lo haga, y se dará cobijo a la comisión de estos hechos en todo el mundo. Esta es la naturaleza de la informática entendida hoy en día como interconectada. El Derecho tiene una dificilísima tarea hoy por hoy para conseguir igualar la velocidad de crucero que lleva el desarrollo tecnológico. Cuestión de difícil solución que va a requerir la unión de grandes juristas, criminólogos, economistas, analistas, etc. para ser capaces de

prever situaciones futuras ahora poco imaginables. También será necesaria la estrecha relación con los profesionales del sector de las telecomunicaciones. Situaciones como la española, que llegó con una década de retraso a la primera regulación penal de estos delitos es inapropiada para combatir efectivamente estas acciones. Si los Estados quieren disponer de herramientas legales suficientes para proteger de este tipo de prácticas tanto a sus ciudadanos y empresas, como a ellos mismos y sus instituciones, deben actuar ahora. Las posibilidades de la informática son infinitas, por tanto las de la delincuencia informática lo son también. Debemos estar preparados y adelantarnos a situaciones que puedan provocar el deterioro de la sociedad que estamos construyendo.

CONCLUSIONES DE LA SEGUNDA PARTE

Los delitos de daños informáticos han adquirido en los últimos años una relevancia desconocida hasta ahora por nuestro ordenamiento penal. Desde su tardía aparición con el Código penal de 1995, hasta su actual configuración tras la entrada en vigor de la LO 5/2010 de 22 de junio han pasado de no existir, a ocupar una posición prácticamente marginal, hasta convertirse en auténticos tipos complejos hoy en día.

La tramitación legislativa entendida en su sentido más amplio (recordemos que la mayor parte de los trabajos de modernización de estos delitos se ha llevado a cabo en el seno de la Comisión General de Codificación) ha concluido con sustanciales cambios. En primer lugar la adaptación el antiguo 264.2 CP a la formulación que se ha venido haciendo en el seno de la Comunidad Internacional, muy especialmente en la Unión Europea a través de la Decisión Marco 2005/222/JAI; en segundo lugar la introducción de un tipo penal inédito en nuestro ordenamiento: el sabotaje informático sobre sistemas informáticos (interrupción u obstaculización), también de acuerdo a la normativa internacional; en tercer lugar se han conformado tipos agravados para los dos anteriores; y por último se ha tipificado expresamente la responsabilidad penal de las personas jurídicas por tales acciones. Así, el actual artículo 264 CP recoge en su mayor parte con acierto el mandato internacional, y dota a nuestro ordenamiento penal de herramientas, al menos suficientes, para combatir este nuevo tipo de criminalidad.

CONCLUSIONES DE LA TERCERA PARTE

Sin embargo, reconociendo las bondades de la actual regulación, a la hora de hacer un análisis crítico en la regulación española se plantean algunos problemas no resueltos. El primero de ellos, y uno de los más importantes, es el relativo a la determinación del bien jurídico protegido por los delitos de daños informáticos. La doctrina más clásica afirma que el único bien jurídico que se protege en este delito de daños es el patrimonio, traducido en el daño a la propiedad ajena. El hecho de realizarse tales ataques por medios informáticos, o contra elementos informáticos, no confiere una naturaleza diferente al bien jurídico protegido. La doctrina más moderna, por el contrario, cree que esta interpretación no es adecuada, pues si bien es cierto que se protegen unos bienes individualizables y concretos, junto a ellos se propone la existencia de un nuevo bien jurídico supraindividual merecedor de protección penal. La realidad ha evolucionado de tal manera que cuando se ataca un sistema informático no sólo se está produciendo un daño concreto para una persona, sino que se está vulnerando un nuevo bien jurídico, cuyo objeto no se ha sabido definir detalladamente todavía, pero que gira en torno a la seguridad de los sistemas informáticos y las redes de comunicaciones. Una sociedad interconectada, como la actual, debe tener un ordenamiento que sea consciente de la importancia de la herramienta que interconecta a la propia sociedad y la proteja, de tal manera que ataques que afecten a la integridad de esa red, no sólo se configuren como daños concretos a usuarios concretos, sino como un perjuicio para toda la sociedad en abstracto.

Sobre la forma de redactar los tipos podemos aventurar algunas conclusiones también. En primer lugar, en relación con los problemas de interpretación que suscitan las acciones de borrar y suprimir recogidas en los tipos. También sobre el catálogo de acciones tipificadas que dificulta la interpretación del precepto: en castellano parece complicado diferenciar las acciones de borrar algo o suprimir algo, y, aunque en esta investigación se han interpretado de modo que puedan ser diferenciadas, convendría redactar el artículo de forma que expusiese claramente la acción que se está sancionando. En esta misma línea nos pronunciamos con el término de hacer inaccesible, al que se le pueden otorgar varios significados, cada

uno de los cuales afectará a la hora de valorar el tipo en su conjunto. Igualmente con el vocablo deteriorar, que como analizamos resulta redundante. Además, la inclusión en el propio catálogo de acciones de la conducta dañar es innecesaria, puesto que dañar sería el concepto general, y la forma concreta de hacerlo serían el resto de las conductas descritas. La inclusión de este término responde más a la tradición a la hora de configurar los delitos de daños en general que a una verdadera necesidad tipológica.

En la misma línea que la conclusión anterior debemos manifestarnos en relación con la ya analizada "doble gravedad" que exigen estos delitos. De un lado, el requisito que exige una manera grave de actuar supone una auténtica indeterminación que la doctrina, con razón, no acaba de abordar acertadamente. La propia expresión es compleja desde el punto de vista semántico de la lengua castellana y para su interpretación jurídica no ayuda precisamente encontrarla rodeada de tantos elementos en los tipos penales. La solución aportada en esta investigación, aunque correcta en nuestra opinión, es sólo una más de las posibles que se puede hacer. Clarificar esta situación no parece tanto un problema de interpretación como de una posible modificación en la redacción del precepto en la línea en que se ha realizado en nuestra propuesta de regulación.

Respecto de la otra exigencia de gravedad, en este caso sobre el resultado, el problema es de otra índole, pues está relacionado con la indeterminación del término. La decisión del legislador de mantener una regulación en la misma línea que la anterior y no establecer un límite objetivo para delimitar la aparición del delito vuelve a obligarnos a depender del estudio que realice la doctrina sobre este extremo, así como de la manera de aplicar el derecho por parte de los tribunales referida al alcance que debe tener dicho concepto, por cuanto ha quedado claro que el límite de 400 euros de los daños clásicos no es aplicable en los daños informáticos. En todo caso, si la actual regulación quiere responder a la doctrina clásica sobre los daños, este resultado grave debe estar vinculado exclusivamente al perjuicio patrimonial directo por la pérdida de la cosa, lo que plantea nuevamente problemas de determinación al encontrarnos ante objetos inmateriales, y en frecuentes casos, de difícil valoración económica.

Para dar respuesta a estos y otros problemas que hemos abordado a lo largo de la investigación, así como cumplir de la forma más exacta con la regulación internacional, hemos propuesto un marco legislativo alternativo completo respecto de los daños informáticos y figuras conexas. Tal proposición, trata de resolver punto a punto cada duda planteada a lo largo del texto. En primer lugar centra su desarrollo en un cambio del prisma desde el que se observan este tipo de conductas, pretendiendo construir un nuevo bien jurídico digno de protección penal: la seguridad en los sistemas de información. Esta construcción, similar a la realizada por el legislador francés en su Código penal -también similar a la del legislador británico o norteamericano en la forma, aunque su sistema descodificado de regulación penal implicaría añadir demasiados matices a esta comparación-, permite por un lado dar respuesta a las dudas que la doctrina siempre ha planteado sobre la incardinación de las acciones de daños informáticos como verdaderos delitos de daños, así como unificar estos delitos con otros conexos que en la actualidad han sido introducidos en otras partes del código (especialmente el acceso ilícito del 197.3 CP), o no han sido introducidos en la reforma penal, incumpliendo el mandato internacional (abuso de dispositivos). Junto a esta nueva visión de los daños informáticos, se construye una proposición que dota a estos delitos agrupados bajo el Título propuesto de "delitos contra la seguridad en los sistemas de información" de completa autonomía en el Código, y sobre el mismo se proponen otras modificaciones menores, especialmente para dar respuesta a los problemas semánticos planteados en la regulación actual, así como unas pautas de interpretación de los elementos bajo este nuevo prisma.

CONCLUSIÓN DE LA INVESTIGACIÓN

No cabe duda de que en la actualidad tanto las instituciones, sean públicas o privadas, como los particulares, y toda clase de asociaciones, tomen la forma que sea, se ven abocados irremediablemente a la utilización de equipos informáticos y sistemas de información. Es simplemente inevitable. Parece difícil volver a una situación anterior tal y como se ha ido produciendo la evolución de la sociedad. Nos guste o no, este es el camino que se ha decidido seguir. Sin embargo, la introducción en la sociedad de nuevas herramientas pensadas para hacer a las personas la vida más

cómoda, supone que puedan ser utilizadas con fines totalmente opuestos para las que fueron creadas, atentos a los cuales deben estar siempre los poderes públicos, tanto en el ámbito nacional como internacional.

La conclusión final que se extrae de la elaboración de este trabajo de investigación es la de que se han puesto en funcionamiento las herramientas legales (e incluso policiales) oportunas para proteger a la sociedad de un nuevo tipo de delincuencia, tanto en el concierto internacional, lo cual es esencial, como en nuestro ordenamiento interno. Sin embargo, la regulación que se ha realizado en España respecto a los delitos de daños informáticos, aunque puede resultar suficiente en el momento actual y es acorde a la mayor parte de los preceptos internacionales y semejante a la de los países de nuestro entorno, puede ser reformulada desde nuevos principios integradores. Las construcciones literales de los tipos arrojan algunas dudas de interpretación, y en la jurisprudencia actual no encontramos respuesta por la escasez de casos planteados ante los Tribunales, pues la existencia de esta clase de delitos que llegan a ser conocidos es todavía escasa. El éxito que supone haber sido conscientes de la nueva problemática aparecida con el desarrollo de las nuevas tecnologías, no debe empañarse por una regulación farragosa, y de difícil interpretación. Si bien se ha comenzado a recorrer el camino para proteger a la sociedad de nuevos tipos de delincuencia, es necesario hacerlo con la máxima efectividad.

Por ello, desde el reconocimiento que debemos profesar por la puesta en marcha de medidas concretas tanto en el ámbito nacional como internacional, debe exhortarse a mantener el esfuerzo actual en completar de la mejor forma nuestro ordenamiento jurídico en relación con las nuevas tecnologías, especialmente en el ámbito penal.

BIBLIOGRAFÍA

Manuales, monografías y artículos citados:

ABBATE, Janet: *Inventing the Internet*, Ed. MIT Press, 1ª edición, Cambridge, 1999.

ABOSO, Gustavo E. y ZAPATA, María F.: *Cibercriminalidad y Derecho penal*, Ed. B de F, 1ª edición, Montevideo, 2006.

ADÁN DEL RÍO, Carmen: "La persecución y sanción de los delitos informáticos" en *Eguzkilore: Cuaderno del Instituto Vasco de Criminología*, nº 20, 2006.

ALAMILLO DOMINGO, Ignacio: "Las políticas públicas en materia de seguridad en la sociedad de la información" en *Revista de Internet, derecho y política. Revista d'internet, dret i política*, nº 9, 2009.

ALONSO GARCÍA, Ricardo: *Sistema Jurídico de la Unión Europea*, Ed. Thomson Reuters, 2ª edición, Navarra, 2010.

ALTAVA LAVALL, Manuel Guillermo: *Lecciones de Derecho Comparado*, Ed. Universitat Jaume I, 1ª edición, Castellón de la Plana, 2003.

ÁLVAREZ GARCÍA, Francisco Javier; MANJÓN-CABEZA OLMEDA, Araceli y VENTURA PÜSCHEL, Arturo (coords.): *La adecuación del Derecho penal español al ordenamiento de la Unión Europea*, Ed. Tirant lo Blanch, 1ª edición, Valencia, 2009.

ÁLVAREZ GARCÍA, Francisco Javier y GONZÁLEZ CUSSAC, José Luis (dirs.): *Comentarios a la Reforma Penal 2010*, Ed. Tirant lo Blanch, 1ª edición, Valencia, 2010.

ÁLVAREZ VIZCAYA, Maite: "Consideraciones político criminales sobre la delincuencia informática: el papel del derecho penal en la red" en *Internet y Derecho penal. Consejo General del Poder Judicial*, nº 10, 2001.

AMADEO GADEA, Sergio (dir.): *Código Penal. Doctrina Jurisprudencial. Parte especial* Ed. Factum Libri Ediciones, Madrid, 2009.

ANDRÉS DOMÍNGUEZ, Ana Cristina: *El Delito de Daños: Consideraciones Jurídico-Políticas y Dogmáticas*, Ed. Universidad de Burgos, 1ª edición, Burgos, 1999.

ANDRÉS DOMÍNGUEZ, Ana Cristina: "Los daños informáticos en la Unión Europea" en *La Ley: Revista jurídica española de doctrina, jurisprudencia y bibliografía*, nº 1, 1999.

ANDRÉS DOMÍNGUEZ, Ana Cristina: "Los daños informáticos en el Derecho penal europeo" en ÁLVAREZ GARCÍA, Francisco Javier; MANJÓN-CABEZA OLMEDA, Araceli y VENTURA PÜSCHEL, Arturo (coords.): *La adecuación del Derecho penal español al ordenamiento de la Unión Europea*, Ed. Tirant lo Blanch, 1ª edición, Valencia, 2009.

ANDRÉS DOMÍNGUEZ, Ana Cristina: "Daños" en ÁLVAREZ GARCÍA, Francisco Javier y GONZÁLEZ CUSSAC, José Luis (dirs.): *Comentarios a la Reforma Penal 2010*, Ed. Tirant lo Blanch, 1ª edición, Valencia, 2010.

ARNALDO ALCUBILLA, Enrique: "El orden público y la seguridad ciudadana en la Constitución española de 1978" en *Cuadernos de Seguridad y Policía*, nº 7, 2011.

AROCENA, Gustavo A.: "De los Delitos Informáticos" en *Revista de la Facultad de Derecho UNC*, vol. 5, nº 1, 1997.

ATKINS, Timothy B.: "La cooperación internacional policial en el ciberespacio" en *Informática y derecho. Revista iberoamericana de derecho informático*, nº 27, 28 y 29, 1998.

BACIGALUPO SAGGESE, Silvina: "Derecho penal y construcción europea" en BACIGALUPO SAGGESE, Silvina y CANCIO MELIÁ, Manuel (coords.): *Derecho penal y política transnacional*, Ed. Atelier, 1ª edición, Barcelona, 2005.

BACIGALUPO SAGGESE, Silvina: "Ética empresarial y Responsabilidad penal de las empresas" en *Encuentros multidisciplinares*, vol. 13, nº 39, 2011.

BACIGALUPO SAGGESE, Silvina: "Los criterios de imputación de la responsabilidad penal de los entes colectivos y de sus órganos de gobierno (arts. 31 bis y 129 CP)" en *La Ley*, nº 7541, 2011.

BACIGALUPO SAGGESE, Silvina y CANCIO MELIÁ, Manuel (coords.): *Derecho penal y política transnacional*, Ed. Atelier, 1ª edición, Barcelona, 2005.

BACIGALUPO ZAPATER, Enrique: *Derecho penal. Parte general*, Ed. Hammurabi, 2ª edición, 1999.

BAJO FERNÁNDEZ, Miguel.: *Compendio de Derecho penal. Parte Especial (volumen I)*, Ed. Centro de Estudios Ramón Areces, 1ª edición, Madrid, 1998.

BAJO FERNÁNDEZ, Miguel y BACIGALUPO SAGGESE, Silvina: *Derecho penal económico*, Ed. Editorial Universitaria Ramón Areces, 2ª edición, Madrid, 2010.

BAKER, Glenn D.: "Trespassers Will Be Prosecuted: Computer Crime in the 1990s" en *Computer Law Journal*, nº 12, 1993.

BALLESTEROS LLOMPART, Jesús: "Filosofía del Derecho, conciencia ecológica y universalismo ético" en *Diálogo filosófico*, nº Enero-Abril, 2003.

BANKS, Michael A.: *On The way to the web: the secret history of the internet and its founders*, Ed. Springer-Verlag, 1ª edición, Nueva York, 2008.

BARRIO ANDRÉS, Moisés: "La ciberdelincuencia en el Derecho español" en *Revista de las Cortes Generales*, nº 83, 2011.

BARRIO ANDRÉS, Moisés: "El régimen jurídico de los delitos cometidos en Internet en el derecho español tras la reforma penal de 2010" en *Delincuencia informática. Tiempos de cautela y amparo*, Ed. Thomson Reuters Aranzadi, 1ª edición, Navarra, 2012.

BARROSO, David: "La radiografía del cibercrimen 2008" en *Seguritecnia: Revista decana independiente de seguridad*, nº 350, 2009.

BARTOLOMÉ CENZANO, José Carlos: *El orden público como límite al ejercicio de los derechos y libertades*, Ed. Centro de estudios políticos y constitucionales, 1ª edición, Madrid, 2002.

BENEDITO AGRAMUNT, José: "Hacia la sociedad de la información" en *Informática y derecho. Revista iberoamericana de derecho informático*, nº 27, 28 y 29, 1998.

BENÍTEZ ORTÚZAR, Ignacio Francisco: *Reformas del Código Penal. Respuestas para una sociedad del Siglo XXI*, Ed. Dykinson, 1ª edición, Madrid, 2009.

BERDUGO GÓMEZ DE LA TORRE, Ignacio: "La reforma de los delitos contra la propiedad industrial" en *Documentación Jurídica*, nº 37-40, 1985.

BEST, Reba A. y PICQUET, Cheryn: *Computer Law and Software Protection: A Bibliography of Crime, Liability, Abuse and Security, 1984 trought 1992*. Ed. Mcfarland, 1ª edición, Londres, 1993.

BORGHELLO, Cristian: *Cronología de los virus informáticos: historia del malware*, Ed. Eset, edición digital, San Diego, 2012.
(http://www.eset-la.com/pdf/prensa/informe/cronologia_virus_informaticos.pdf).

BUENO ARÚS, Francisco: "El delito informático*"* en *Actualidad Informática Aranzadi*, nº 11, 1994.

BUSTOS PUECHE, José Enrique: "Incontinencia legislativa, pobreza de resultados" en *Anuario de la Facultad de Derecho de Alcalá de Henares*, s/n, 2006.

CALONGE VELÁZQUEZ, Antonio: "Sistema competencial y de fuentes en el espacio de libertad, seguridad y justicia" en *Revista de derecho de la Unión Europea*, nº 10, 2006.

CAMACHO LOSA, Luis: *El delito informático*, Ed. Madrid, 1ª edición, Madrid, 1987.

CAMPBELL-KELLY, Martin y ASPRAY, William: *Computer: a history of the information machine*, Ed. Westview Press, 2ª edición, Boulder, 2004.

CARBONELL MATEU, Juan Carlos: "La reforma del tratamiento penal de la seguridad vial" en MORILLAS CUEVA, Lorenzo (dir.): *Delincuencia en materia de tráfico y seguridad vial*, Ed. Dykinson, 1ª edición, Madrid, 2008.

CARBONELL MATEU, Juan Carlos; DEL ROSAL BLASCO, Bernardo; MORILLAS CUEVA, Lorenzo; ORTS BERENGUER, Enrique y QUINTANAR DÍEZ, Manuel (coords.): *Estudios penales en homenaje al profesor Cobo del Rosal*, Ed. Dykinson, 1ª edición, Madrid, 2006.

CÁRDENAS ARAVENA, Claudia Marcela: "El lugar de comisión de los denominados ciberdelitos" en *Política Criminal: Revista Electrónica Semestral de Políticas Públicas en Materias Penales*, nº 6, 2008.

CARRASCOSA LÓPEZ, Valentín: "¿Es necesaria una legislación mundial para Internet?" en *Informática y derecho. Revista iberoamericana de derecho informático*, nº 27, 28 y 29, 1998.

CERUZZI, Paul E.: *A History of Modern Computing*, Ed. MIT Press, 2ª edición, Cambridge, 2003.

CHICHARRO LÁZARO, Alicia: "La labor legislativa del Consejo de Europa frente a la utilización de Internet con fines terroristas" en *Revista de Internet, derecho y política. Revista d'internet, dret i política*, nº 9, 2009.

CHOCLÁN MONTALVO, José Antonio: *El delito continuado*, Ed. Marcial Pons, 1ª edición, Madrid, 1997.

CLOUGH, Bryan y MUNGO, Paul: *Los piratas del chip: la mafia informática al desnudo*, Ed. Ediciones B, 1ª edición, Barcelona, 1992.

COHEN, Frederick B.: "Computer Viruses - Theory and Experiments" en *Journal Computers and Security*, Ed. Elsevier Sciencie Publishers, nº 6, 1987. (http://all.net/books/virus/index.html).

COHEN, Frederick B.: "Cyber-risks and critical infrastructures" en *Strategic Security*, vol. 27, nº 2, 2003.

COTINO HUESO, Lorenzo: *Libertad en Internet. La red y las libertades de expresión e información*, Ed. Tirant lo Blanch, 1ª edición, Valencia, 2007.

CONSENTINO, Guillermo; GARCÍA, José Alberto; TEJERO, Néstor Fabián y TEJERO, Daniel Omar: "Tras los pasos de la Seguridad perdida. Delitos informáticos" en *Informática y derecho. Revista iberoamericana de derecho informático*, nº 23, 24, 25 y 26, 1998.

CONTRERAS CLUNES, Alberto: "Delitos informáticos: un importante precedente" en *Ius et Praxis*, vol. 9, nº 1, 2003.

CORCOY BIDASOLO, Mirentxu: "Protección penal del sabotaje informático. Especial Consideración de los delitos de daños*"* en *La Ley*, número 1, 1990.

CORCOY BIDASOLO, Mirentxu: "Problemática de la persecución penal de los denominados delitos informáticos: particular referencia a la participación criminal y al ámbito espacio temporal de comisión de los hechos" en *Eguzkilore: cuaderno del Instituto Vasco de Criminología*, nº 21, 2007.

CORCOY BIDASOLO, Mirentxu y JOSHI JUBERT, Ujala: "Delitos contra el patrimonio cometidos por medios informáticos" en *Revista Jurídica de Catalunya*, vol. 87, nº 3, 1988.

CRUZ DE PABLO, José Antonio: *Derecho penal y nuevas tecnologías. Aspectos Sustantivos*, Ed. Grupo Difusión, 1ª edición, Madrid, 2006.

DAVARA RODRÍGUEZ, Miguel Ángel: *Manual de Derecho Informático*, Ed. Thomson Aranzadi, 10ª Edición, Navarra, 2008.

DAVIS, Martin: *Universal computer. The road from Leibniz to Turing*, Ed. W.W. Norton & Company, 1ª edición, Nueva York, 2000.

DE ESTEBAN ALONSO, Jorge y GONZÁLEZ-TREVIJANO SÁNCHEZ, Pedro José: *Tratado de Derecho Constitucional II*, Ed. Universidad Complutense Madrid, 2ª edición, Madrid, 2004.

DE LA CUESTA ARZAMENDI, José Luis y DE LA MATA BARRANCO, Norberto Javier: *Derecho Penal Informático*, Ed. Thomson Reuters, 1ª edición, Navarra, 2010.

DE LA MATA BARRANCO, Norberto Javier: "Utilización abusiva de cajeros automáticos: apropiación de dinero mediante la tarjeta sustraída a su titular" en *Poder Judicial* núm. nº IX (especial), 1988.

DE LA MATA BARRANCO, Norberto Javier: "El delito de daños a datos, programas, documentos y sistemas informáticos*"* en JUANES PECES, Ángel (dir.): *Reforma del Código Penal. Perspectiva Económica tras la entrada en vigor de la LO 5/2010 de 22 de junio. Situación jurídico-penal del empresario*, Ed. El Derecho, 1ª edición, Madrid, 2010.

DE LA MATA BARRANCO, Norberto Javier y HERNÁNDEZ DÍAZ, Leyre: "El delito de daños informáticos. Una tipificación defectuosa" en *Estudios penales y criminológicos*, nº 29, 2009.

DELGADO AGUADO, Juan: "El orden público: proceso evolutivo" en *Cuadernos de Seguridad y Policía*, nº 7, 2011.

DELTA, George B. y MATSUURA, Jeffrey H: *Law of the Internet*, Ed. Aspen Publishers, 2ª edición revisada, Nueva York, 2008.

DEVEZE, Jean: "La fraude informatique, Aspects juridiques" en *La Semaine Juridique*, nº 3289, 1987.

DEVEZE, Jean: "Commentaire de la Loi nº 88-19 du 5 janvier 1988 relative à la fraude informatique" en *Lamy droit de l'informatique*, nº febrero, 1988.

DEMBOWSKI, Klaus: *Gran libro de Hardware: Información sobre la totalidad del hardware, de rápido acceso*. Ed. Marcombo. 2ª edición, Barcelona 2003.

DÍAZ GÓMEZ, Andrés: "El delito informático, su problemática y la cooperación internacional como paradigma de su solución: El Convenio de Budapest" en *REDUR*, nº 8 - diciembre, 2010.

DÍAZ SÁEZ, Vicente: "Ataques DDoS: el 'backstage' de gran parte del cibercrimen" en *Red seguridad: revista especializada en seguridad informática, protección de datos y comunicaciones*, nº 58, 2012.

DIEGO DÍAZ-SANTOS, María Rosario y SÁNCHEZ LÓPEZ, Virginia (coords.): *Hacia un Derecho penal sin fronteras*, Ed. Colex, 1ª edición, Madrid, 2000.

DÍEZ RIPOLLÉS, José Luis: *La racionalidad de las leyes penales*, Ed. Trotta, 1ª edición, Madrid, 2003.

DÍEZ RIPOLLÉS José Luis; ROMEO CASABONA, Carlos María; GRACIA MARTÍN, Luis e HIGUERA GUIMERÁ, Juan Felipe (coords.): *La ciencia del Derecho penal ante el nuevo siglo. Libro homenaje al profesor doctor don José Cerezo Mir*, Ed. Tecnos, 1ª edición, Madrid, 2002.

DOPICO GÓMEZ-ALLER, Jacobo: *Omisión e injerencia en Derecho Penal*, Ed. Tirant lo Blanch, 1ª edición, Valencia, 2006.

EBERHARD, Johann August y ECKHART, Johann Georg: *Leibniz-Biographien*, Ed. Olms, 2ª edición, Hildesheim, 2003.

ELTRINGHAM, Scott: *Prosecuting Computer Crimes*, Ed. US Department of Justice, 1ª edición, Washington DC, 2007.

ESCUDERO MORATALLA, José Francisco; FRIGOLA VALLINA, Joaquín y GANZENMÜLLER ROIG, Carlos: *Delitos contra el orden público, terrorismo, contra el Estado o la Comunidad Internacional*, Ed. Bosch, 1ª edición, Barcelona, 1998.

FAITH CRANOR, Lorrie: "Delincuencia informática" en *Investigación y ciencia*, nº 402, 2010.

FARALDO CABANA, Patricia: "Los conceptos de manipulación informática y artificio semejante en el delito de estafa informática" en *Eguzkilore: Cuaderno del Instituto Vasco de Criminología*, nº 21, 2007.

FARALDO CABANA, Patricia: *Las nuevas técnologías en los delitos contra el patrimonio y el orden socioeconómico*, Ed. Tiran Lo Blanch, 1ª edición, Valencia, 2009.

FARALDO CABANA, Patricia: "Defraudación de telecomunicaciones y uso no consentido de terminales de telecomunicación. Dificultades de delimitación entre los arts. 255 y 256 CP" en MUÑOZ CONDE, Francisco; LORENZO SALGADO, José Manuel; FERRÉ OLIVÉ, Juan Carlos; BECHIARELLI, Emilio Cortés y NÚÑEZ PAZ, Miguel Ángel (dirs.): *Un Derecho penal comprometido. Libro homenaje al Prof. Dr. Gerardo Landrove Díaz*, Ed. Tirant lo Blanch, 1ª edición, Valencia, 2011.

FERNÁNDEZ FERNÁNDEZ, Carmen: "Delitos informáticos" en *Base Informática*, nº 43, 2009.

FERNÁNDEZ LÁZARO, Fernando: "La Brigada de Investigación Tecnológica: la investigación policial" en VELASCO NÚÑEZ, Eloy (dir.): *Delitos contra y a través de las nuevas tecnologías. ¿Cómo reducir su impunidad?*, Ed. Consejo General del Poder Judicial, Cuadernos de Derecho Judicial, 1ª edición, Madrid, 2006.

FERNÁNDEZ-MIRANDA CAMPOAMOR, Alfonso y FERNÁNDEZ-MIRANDA CAMPOAMOR, Carmen: *Sistema electoral, partidos políticos y parlamento*, Ed. Colex, 2ª edición, Madrid, 2008.

FERNÁNDEZ ORDÓÑEZ, Miguel Ángel; CREMADES GARCÍA, Javier e ILLESCAS ORTIZ, Rafael (coords.): *Régimen Jurídico de Internet*, Ed. La Ley, 1ª edición, Madrid, 2001.

FERNANDEZ PALMA, Rosa y MORALES GARCÍA, Oscar: "El delito de daños informáticos y el caso *Hispahack*" en *La Ley. Revista Jurídica Española de Doctrina, Jurisprudencia y Legislación*, nº 1, 2000.

FERNÁNDEZ SANTIAGO, Arturo y CASTRO FUERTES, Marta: "Comentario al artículo 197 CP" en AMADEO GADEA, Sergio (dir.): *Código Penal. Doctrina Jurisprudencial. Parte especial* Ed. Factum Libri Ediciones, Madrid, 2009

FERNÁNDEZ TERUELO, Javier Gustavo: *Cibercrimen. Los delitos cometidos a través de internet*, Ed. Constitutio Criminalis Carolina, 1ª edición, Oviedo, 2007.

FLORES PRADA, Ignacio: *Criminalidad Informática. Aspectos sustantivos y procesales*, Ed. Tirant lo Blanch, 1ª edición, Valencia, 2012.

FOGGETTI, Nadina: "Análisis de un supuesto de delincuencia informática trasnacional" en *Novática. Revista de la Asociación de Técnicos de Informática*, nº 166, 2003.

GALÁN MUÑOZ, Alfonso: "Expansión e intensificación del derecho penal de las nuevas tecnologías: un análisis crítico de las últimas reformas legislativas en materia de criminalidad informática" en *Revista de Derecho y proceso penal*, nº 15, 2006.

GALÁN MUÑOZ, Alfonso: "La internacionalización de la represión y la persecución de la criminalidad informática: un nuevo campo de batalla en la eterna guerra entre prevención y garantías penales" en *Revista penal*, nº 24, 2009.

GALINDO GARCÍA, Ángel: "Ética e Internet: una apuesta a favor de la verdad y de la solidaridad comunicativas", en *Salmanticensis, Universidad Pontificia de Salamanca*, nº. 44.2, 1997.

GALLARDO ORTIZ, Miguel Ángel: *Ámbito jurídico de las tecnologías de la información*, Ed. CGPJ, 1ª edición, Madrid, 1996.

GALLARDO RUEDA, Alberto: "Delincuencia informática: la nueva criminalidad de fin de siglo" en *Cuadernos de política criminal*, nº 65, 1998.

GARCÍA, Mario: "La nueva cara del cibercrimen" en *Byte España*, nº 196, 2012.

GARCÍA DE ENTERRÍA, Eduardo: *Justicia y Seguridad Jurídica en un Mundo de Leyes Desbocadas*, Ed. Civitas, 1ª edición Madrid, 1999 (reimpresión de 2006).

GARCÍA DE ENTERRÍA, Eduardo y FERNÁNDEZ RODRÍGUEZ, Tomás Ramón: *Curso de Derecho administrativo. Tomo I*, Ed. Civitas, 15ª edición, Madrid, 2011.

GARCÍA-ESCUDERO MÁRQUEZ, Piedad: "Consideraciones sobre la iniciativa legislativa del Gobierno*"* en *Cuadernos de Derecho público*, nº 8, 1999.

GARCÍA-ESCUDERO MÁRQUEZ, Piedad: *La iniciativa legislativa del Gobierno*, Ed. Centro de estudios políticos y constitucionales, 1ª edición, Madrid, 2000.

GARCÍA-ESCUDERO MÁRQUEZ, Piedad: "Nociones de técnica legislativa para uso parlamentario" en *Revista Parlamentaria de la Asamblea de Madrid*, nº 13, 2005.

GARCÍA-ESCUDERO MÁRQUEZ, Piedad: *El procedimiento legislativo ordinario en las Cortes Generales*, Ed. Centro de Estudios Políticos y Constitucionales, 1ª edición, Madrid, 2006.

GARCÍA-ESCUDERO MÁRQUEZ, Piedad: *Manual de técnica legislativa*, Ed. Civitas, 1ª edición, Madrid, 2011.

GARCÍA GARCÍA-CERVIGÓN, Josefina: "Daños informáticos. Consideraciones penales y criminológicas" en *Actualidad Jurídica Aranzadi*, nº 588, 2003.

GARCÍA MEXÍA, Pablo: *Principios de Derecho de Internet*, Ed. Tirant lo Blanch, 2ª edición, Valencia, 2005.

GARCÍA ROCA, Javier y SANTOLAYA MACHETTI, Pablo (dirs.): *La Europa de los Derechos. El Convenio Europeo de Derechos Humanos*, Ed. Centro de Estudios Políticos y Constitucionales, 2º edición, Madrid, 2009.

GARRIDO MAYOL, Vicente: *Las garantías del procedimiento prelegislativo: la elaboración y aprobación de los proyectos de ley*, Ed. Tirant lo Blanch, 1ª edición, Valencia, 2010.

GARCÍA-PABLOS DE MOLINA, Antonio: *Introducción al Derecho Penal*, Ed. Universitaria Ramón Aceres, 4º edición, Madrid, 2006.

GIL GIL, Alicia; LACRUZ LÓPEZ, Juan Manuel; MELENDO PARDOS, Mariano y NÚÑEZ FERNÁNDEZ, José: *Curso de Derecho penal. Parte General*, Ed. Dykinson, Madrid, 2011.

GIL GIL, Alicia: "Unidad y pluralidad de delitos" en GIL GIL, Alicia; LACRUZ LÓPEZ, Juan Manuel; MELENDO PARDOS, Mariano y NÚÑEZ FERNÁNDEZ, José: *Curso de Derecho penal. Parte General*, Ed. Dykinson, Madrid, 2011.

GOLDSTINE, Herman Heine: *The Computer, from Pascal to Von Neumann*, Ed. Princeton University Press, 5ª edición, Nueva Jersey, 1993.

GÓMEZ MARTÍN, Víctor: "Sabotaje informático, 'top manta', importaciones paralelas y fraude de inversores: ¿algunos exponentes de un nuevo derecho Penal económico?" en *Revista Jurídica de Catalunya*, nº 4, 2011.

GONZÁLEZ, Encarna: "El cibercrimen, una amenaza en ciernes" en *Pc World*, nº 251, 2008.

GONZÁLEZ HURTADO, Jorge Alexandre: *Aproximación a la fase prelegislativa en la elaboración de normas penales. La Comisión General de Codificación y el Derecho penal en la actualidad*, Ed. Dykinson, 1ª edición, Madrid, 2013.

GONZÁLEZ ORDOVÁS, María José: *Ineficacia, anomia y fuentes del derecho*, Ed. Dykinson, 1ª edición, Madrid, 2003.

GONZÁLEZ RUS, Juan José: "Tratamiento penal de los ilícitos patrimoniales relacionados con medios o procedimientos informáticos" en *Separata de Jornadas de estudio sobre nuevas formas de delincuencia*, 28 a 30 Noviembre 1988.

GONZÁLEZ RUS, Juan José: "Protección penal de sistemas, elementos, datos, documentos y programas informáticos" en *Revista Electrónica de Ciencia Penal y Criminología*, nº 1, 1999.

GONZÁLEZ RUS, Juan José: "Naturaleza y ámbito de aplicación del delito de daños en elementos informáticos" en DÍEZ RIPOLLÉS José Luis; ROMEO CASABONA, Carlos María; GRACIA MARTÍN, Luis e HIGUERA GUIMERÁ, Juan Felipe (coords.): *La ciencia del Derecho penal ante el nuevo siglo. Libro homenaje al profesor doctor don José Cerezo Mir*, Ed. Tecnos, 1ª edición, Madrid, 2002.

GONZÁLEZ RUS, Juan José: "El cracking y otros supuestos de sabotaje informático" en *Estudios Jurídicos. Ministerio Fiscal*, nº 2, 2003.

GONZÁLEZ RUS, Juan José: "Daños a través de Internet y denegación de servicios" en JORGE BARREIRO, Agustín (coord.): *Homenaje al profesor Dr. Gonzalo Rodríguez Mourullo*, Ed. Thomson Civitas, 1ª edición, Navarra, 2005.

GONZÁLEZ RUS, Juan José: "Los ilícitos en la red (I): hackers, crackers, cyberpunks, sniffers, denegación de servicio y otros comportamientos semejantes" en ROMEO CASABONA, Carlos María (dir.): *El cibercrimen, nuevos retos jurídico-penales, nuevas respuestas político criminales*, Ed. Comares, Granada, 2006.

GUANARTEME SÁNCHEZ LÁZARO, Fernando: "Alarma social y Derecho penal" en ROMEO CASABONA, Carlos María; GUANARTEME SÁNCHEZ LÁZARO, Fernando y ARMAZA ARMAZA, Emilio José (coords.): *La adaptación del Derecho penal al desarrollo tecnológico*, Ed. Comares, 1ª edición, Granada, 2010.

GUERRERO, Diego: *Fraude en la red*, Ed. Ra-Ma, 1ª edición, Madrid, 2010.

GUTIÉRREZ FRANCÉS, María Luz: *Fraude Informático y Estafa*, Ed. Ministerio de Justicia, 1ª edición, Madrid, 1991.

GUTIÉRREZ FRANCÉS, María Luz: "Computer Crime and Other Crimes against Information Technology in Spain" en AIDP: "Computer Crime and Other Crimes Aganits Informátion Technology" en *Internacional Review of Penal Law*, Ed. Erès, nº 64, 1º y 2º trimestres, 1993.

GUTIÉRREZ FRANCÉS, María Luz.: "Delincuencia económica e informática en el nuevo Código Penal", en GALLARDO ORTIZ, Miguel Ángel: *Ámbito jurídico de las tecnologías de la información*, Ed. CGPJ, 1ª edición, Madrid, 1996.

GUTIÉRREZ FRANCÉS, María Luz: "Reflexiones sobre la ciberdelincuencia hoy. En torno a la ley penal en el espacio virtual" en *Revista electrónica del departamento de derecho de la Universidad de La Rioja, REDUR*, nº 3, 2005.

HEFENDEHL, Roland (dir.), edición española a cargo de ALCÁCER GUIRAO, Rafael; MARTÍN LORENZO, María y ORTIZ DE URBINA GIMENO, Íñigo: *La teoría del bien jurídico ¿Fundamento de legitimación del Derecho penal o juego de abalorios dogmáticos?*, Ed. Marcial Pons, 1ª edición, Madrid, 2007.

HEREDERO HIGUERAS, Manuel: "Los delitos informáticos en el proyecto de código penal de 1994" en *Informática y derecho. Revista iberoamericana de derecho informático*, nº 12, 13, 14 y 15, 1996.

HERNÁNDEZ CALLEJA, Ricardo: "Cibercrimen, crónica de un auge anunciado" en *Pc World*, nº 269, 2009.

HERRÁN ORTIZ, Ana Isabel: *El Derecho a la intimidad en la nueva ley orgánica de protección de datos personales*, Ed. Dykinson, 1ª edición, 2002.

HIMANEN, Pekka: *La ética del hacker y el espíritu de la era de la información*, Ed. Destino, 1ª edición, Barcelona, 2002.

HÖRNLE, Tatjana: "La protección de sentimientos en el STGB" en HEFENDEHL, Roland: *La teoría del bien jurídico ¿Fundamento de legitimación del Derecho penal o juego de abalorios dogmáticos?*, Ed. Marcial Pons, 1ª edición, Madrid, 2007.

HUETE NOGUERAS, Javier: "La reforma de los delitos informáticos" en *Diario La Ley*, nº 7534, 2010.

HUERTA TOCILDO, Susana: *Principales novedades de los delitos de omisión en el Código penal de* 1995, Ed. Tirant lo Blanch, 1ª edición, Valencia, 1997.

HUERTA TOCILDO, Susana: "Principio de legalidad y normas sancionadoras" en *El principio de legalidad. Actas de las V Jornadas de la Asociación de Letrados del Tribunal Constitucional*, Ed. Centro de Estudios Políticos y Constitucionales, 1ª edición, Madrid, 2000.

HUERTA TOCILDO, Susana: "Artículo 25.1. El Derecho a la legalidad penal" en *Comentarios a la Constitución Española en su XXX Aniversario*, Ed. Wolters Kluwert, 1ª edición, Madrid, 2009.

HUERTA TOCILDO, Susana: "El contenido debilitado del principio europeo de legalidad penal" en GARCÍA ROCA, Javier y SANTOLAYA MACHETTI, Pablo: *La Europa de los Derechos. El Convenio Europeo de Derechos Humanos*, Ed. Centro de Estudios Políticos y Constitucionales, 2º edición, Madrid, 2009.

HUERTA TOCILDO, Susana y ANDRÉS DOMÍNGUEZ, Cristina: "Intimidad e informática" en *Revista de Derecho penal*, nº 6, 2002.

HUGHES, Lorine A. y DE LONE, Gregory J.: "Virus, Worms, and Trojan Horses. Serious Crimes, Nuisance or both?" en *Social Science Computer Review*, vol. 25, nº 1, 2007.

HYMAN, Anthony: *Charles Babbage: pioneer of the computer*, Ed. Princeton University Press, 1ª edición, Nueva Jersey, 1985.

JAEGER, Marc: "La fraude informatique" en *Revue de Droit Penal et de Criminologie*, nº 65, 1985.

JAKOBS, Günther, edición española a cargo de CUELLO CONTRERAS, Joaquín y SERRANO GONZÁLEZ DE MURILLO, José Luis: *Derecho penal. Parte general. Fundamentos y teoría de la imputación*, Ed. Marcial Pons, 2ª edición (corregida), Madrid, 1997.

JAN DRIJBER, Berend: "Enfoque común hacia el crimen organizado: el caso de la Unión Europea" en *Informática y derecho. Revista iberoamericana de derecho informático*, nº 27, 28 y 29, 1998.

JORGE BARREIRO, Agustín (coord.): *Homenaje al profesor Dr. Gonzalo Rodríguez Mourullo*, Ed. Thomson Civitas, 1ª edición, Navarra, 2005.

JUANES PECES, Ángel (dir.): *Reforma del Código Penal. Perspectiva Económica tras la entrada en vigor de la LO 5/2010 de 22 de junio. Situación jurídico-penal del empresario*, Ed. El Derecho, 1ª edición, Madrid, 2010.

KELLY, Dennis J. y MASTROCOLA, Paul R.: "The Economic Espionage Act of 1996" en *New England journal on criminal and civil confinement*, nº 26, 2000.

KERR, Orrin S.: "Internet surveillance law after the USA patriot Act: the big brother that isn't" en *Northwestern University Law Review*, nº 97, 2003.

KURTZ, Gerardo; MCCLURE, Stuart y SCAMBRAY, Joel: *Hackers 2. Secretos y soluciones para la seguridad de redes*, Ed. Mcgraw-Hill, 1ª edición, Madrid, 2001.

LAGARES GARCÍA, Diego: *Internet y Derecho*, Ed. Carena, 1ª edición, Barcelona, 2000.

LANDA DURÁN, Graciela Margarita: "Los delitos informáticos en el Derecho penal de México y España" en *Revista del Instituto de la Judicatura Federal*, número 24, 2007.

LAPIEDRA ALCAMÍ, Rafael: "Diferencia entre Sistema Informático y Sistema de Información" en *Cámara de Comercio de Valencia-Artículos Empresariales*, nº 3-1454-10-2002, 2002.

LARKIN, Erik: "Cibercrimen. Delincuentes profesionales online" en *Pc World*, nº 224, 2005.

LEZERTUA RODRÍGUEZ, Manuel: "El Proyecto de Convenio sobre el cibercrimen del Consejo de Europa - proteger el ejercicio de derechos fundamentales en las redes informáticas" en *Cuadernos europeos de Deusto*, nº 25, 2001.

LITTLEJOHN SHINDER, Debra: *Prevención y detección de delitos informáticos*, Ed. Anaya, 1ª edición, Madrid, 2003.

LOBO GONZÁLEZ, Raquel y ÁLVAREZ RODRÍGUEZ, Mabel: "Comentario al artículo 268 CP" en AMADEO GADEA, Sergio (dir.): *Código Penal. Doctrina Jurisprudencial. Parte especial*, Ed. Factum Libri Ediciones, Madrid, 2009.

LÓPEZ, Antonio: "La investigación policial en Internet: estructuras de cooperación internacional" en R*evista de Internet, derecho y política. Revista d'internet, dret i política*, nº 5, 2007.

LÓPEZ CALERA, Nicolás María (coord.): La palabra contra el terrorismo, Ed. Universidad de Granada, 1ª edición, Granada, 2004.

LÓPEZ ORTEGA, Juan José: "La admisibilidad de los medios de investigación basados en registros informáticos" en *Cuadernos de derecho judicial*, nº 9, 2002.

LÓPEZ-VIDRIERO TEJEDOR, Icíar: *Delitos Informáticos ¿Cuáles son? ¿Cómo denunciarlos?*, 2011, (http://www.microsoft.com/business/smb/es-es/legal/delitos_informaticos.mspx).

MAGDALENA, Nicolás: "El cibercrimen" en *Escritura pública*, nº 16, 2002.

MAGRO SERVET, Vicente: "La delincuencia informática. ¿Quién Gobierna Internet?" en *Diario La Ley*, nº 6077, 2004.

MANSFIELD, Richard: *Defensa contra hackers. Protección de información privada*, Ed. Anaya, 1ª edición, Madrid, 2001.

MARCHENA GÓMEZ, Manuel: "Jurisdicción e Internet", en *Conferencia XV años de encuentro sobre Informática y Derecho*, Ed. Universidad Pontificia Comillas, Madrid, 2001.

MARCHENA GÓMEZ, Manuel: "El sabotaje informático: entre los delitos de daños y los desórdenes públicos*"* en *Internet y Derecho penal. Consejo General del Poder Judicial*, número 10, Madrid, 2001.

MATA y MARTÍN, Ricardo Manuel: *Delincuencia informática y derecho penal*, Ed. Edisofer, 1ª edición, Madrid, 2001.

MATA y MARTÍN, Ricardo Manuel: "Criminalidad informática: una introducción al cibercrimen" en *Actualidad penal*, nº 36, 2003.

MATA y MARTÍN, Ricardo Manuel: "Protección penal de la propiedad intelectual y servicios de radiodifusión e interactivos: excesos y equívocos. Su continuación en la reforma de 25 de noviembre de 2003".

MATAS GARCÍA, Abel Mariano; MÍGUEZ PÉREZ, Carlos; PÉREZ AGUDÍN, Justo; PICOUTO RAMOS, Fernando y RAMOS VARÓN, Antonio Ángel: *La biblia del Hacker. Edición 2006*, Ed. Anaya Multimedia, 1ª edición, Madrid, 2006.

MATELLANES RODRÍGUEZ, Nuria: "Algunas notas sobre las formas de delincuencia informática en el Código Penal" en DIEGO DÍAZ-SANTOS, María Rosario y SÁNCHEZ LÓPEZ, Virginia (coords.): *Hacia un Derecho penal sin fronteras*, Ed. Colex, 1ª edición, Madrid, 2000.

MAZA MARTÍN, José Manuel: "La necesaria reforma del Código Penal en materia de Delincuencia Informática" en *Estudios Jurídicos. Ministerio Fiscal*, nº 2, 2003.

MAZUELOS COELLO, Julio Fernando: "Consideraciones sobre el delito de daños informáticos, en especial sobre la difusión de virus informáticos" en *Derecho Penal y Criminología: Revista del Instituto de Ciencias Penales y Criminológicas*, vol. 28, nº 85, 2007.

MELL, Patricia: "Big Brother at the Door: Balancing National Security with Privacy Under the USA Patriot Act" en *Denver University Law Review*, nº 80, 2002.

MENÉNDEZ MENÉNDEZ, Aurelio (dir.): *La proliferación legislativa: un desafío para el Estado de Derecho*, Ed. Thomson Civitas, 1ª edición, Madrid, 2004.

MESTRE DELGADO, Juan Francisco: "Sobre el valor de la jurisprudencia en Derecho español" en *Revista General de Derecho Público Comparado*, nº 3, 2008.

MIGUEL MOLINA, María del Rosario y OLTRA GUTIÉRREZ, Juan Vicente: *Deontología y aspectos legales de la informática: cuestiones éticas, jurídicas y técnicas básicas*, Ed. Universidad Politécnica de Valencia, 1ª edición, 2007.

MIR PUIG, Santiago: "Bien Jurídico y Bien Jurídico-Penal como Límites del *Ius Puniendi*" en *Estudios penales y criminológicos*, nº 14, 1991.

MIR PUIG, Santiago: *Delincuencia Informática*, Ed. PPU, 1ª edición, Barcelona, 1992.

MIR PUIG, Santiago: *Derecho Penal. Parte General*, Ed. Reppertor, 8ª edición, Barcelona, 2010.

MIRÓ LLINARES, Fernando: "Delitos informáticos: Hacking. Daños" en ORTIZ DE URBINA GIMENO, Íñigo (coord.): *Memento Experto. Reforma Penal*, Ed. Ediciones Francis Lefebvre, 1ª edición, Madrid, 2010.

MOLINA GIMENO, Francisco Javier: "El hacking ¿una conducta punible?" en *Diario La Ley*, nº 7131, 2009.

MONTERDE FERRER, Francisco: "Especial consideración de los atentados por medios informáticos contra la intimidad y privacidad" en VELASCO NÚÑEZ, Eloy (dir.): *Delitos contra y a través de las nuevas tecnologías. ¿Cómo reducir su impunidad?*, Ed. Consejo General del Poder Judicial, Cuadernos de Derecho Judicial, 1ª edición, Madrid, 2006.

MOORE, Robert: *Cybercrime: Investigating High Technology Computer Crime*, Ed. Elsevier, 2ª edición, Nueva York, 2010.

MORAL TORRES, Anselmo: "Colaboración policial internacional en el ciberespacio" en *Informática y derecho. Revista iberoamericana de derecho informático*, nº 27, 28 y 29, 1998.

MORALES GARCÍA, Óscar: "Apuntes de política criminal en el contexto tecnológico. Una aproximación a la convención del Consejo de Europa sobre Cyber-Crime" en *Cuadernos de derecho judicial*, nº 9, 2002.

MORALES GARCÍA Óscar: "Comentario a los delitos informáticos de los arts. 197, 248 y 264 CP" en VV.AA: *Delincuencia informática. Tiempos de cautela y amparo,* Ed. Thomson Reuters Aranzadi, 1ª edición, Navarra, 2012.

MORENÉS ÁLVAREZ DE EULATE, Pedro: "Nuevas tecnologías y seguridad. El tratado de Budapest, un paso más" en *Economista*, nº 91, 2002.

MORILLAS CUEVA, Lorenzo: "Nuevas tendencias del Derecho Penal: Una reflexión dirigida a la cibercriminalidad" en *Cuadernos de política criminal*, nº 94, 2008.

MORILLAS CUEVA, Lorenzo (dir.): *Delincuencia en materia de tráfico y seguridad vial*, Ed. Dykinson, 1ª edición, Madrid, 2008.

MORILLAS CUEVA, Lorenzo y CRUZ BLANCA, María José: *Informática y delito. Aspectos penales relacionados con las nuevas tecnologías* en BENÍTEZ ORTÚZAR, Ignacio Francisco: *Reformas del Código Penal. Respuestas para una sociedad del Siglo XXI,* Ed. Dykinson, 1ª edición, Madrid, 2009.

MOYA FUENTES, María del Mar: "La alteración y duplicación del número identificativo de equipos de telecomunicaciones, su comercialización y su utilización: art. 286.2 y 4 CP" en *Revista Electrónica de Ciencia Penal y Criminología*, nº 11-2, 2009, (http://criminet.ugr.es/recpc/11/recpc11-02.pdf).

MUÑOZ CONDE, Francisco: *Derecho Penal, Parte Especial,* Ed. Tirant lo Blanch, 18ª edición, Valencia, 2010.

MUÑOZ CONDE, Francisco y GARCÍA ARÁN, Mercedes: *Derecho Penal, Parte General,* Ed. Tirant lo Blanch, 8ª edición, Valencia, 2010.

MUÑOZ CONDE, Francisco; LORENZO SALGADO, José Manuel; FERRÉ OLIVÉ, Juan Carlos; BECHIARELLI, Emilio Cortés y NÚÑEZ PAZ, Miguel Ángel (dirs.): *Un Derecho penal comprometido. Libro homenaje al Prof. Dr. Gerardo Landrove Díaz*, Ed. Tirant lo Blanch, 1ª edición, Valencia, 2011.

MUÑOZ MACHADO, Santiago: *La regulación de la red, Poder y derecho en internet*, Ed. Taurus, 1ª edición, Madrid, 2000

NAVA GARCÉS, Alberto Enrique: *Delitos informáticos*, Ed. Editorial Porrúa, 2ª edición, México D.F., 2007.

NIELSEN, Michael A. y CHUANG, Isaac L: *Quantum Computation and Quantum Information*, Ed. Cambridge University Press, 10ª edición, 2011.

NIMMER, Raymond T.: *Law of Computer Technology*, Ed. Thomson Reuters, 4ª edición, Nueva York, 2012.

NORA, Dominique: *La Conquista Del Ciberespacio*, Ed. Andrés Bello, 1ª edición, Barcelona, 1997.

NÚÑEZ FERNÁNDEZ, José: "Algunos aspectos conceptuales y políticos de la criminalidad de cuello blanco" en *Cuardernos de Político Criminal*, nº 71, 2000.

NÚÑEZ FERNÁNDEZ, José: "Aplicación y determinación de la pena" en GIL GIL, Alicia, LACRUZ LÓPEZ, Juan Manuel, MELENDO PARDOS, Mariano y NÚÑEZ FERNÁNDEZ, José: *Curso de Derecho penal. Parte General*, Ed. Dykinson, Madrid, 2011.

NÚÑEZ FERNÁNDEZ, José: "Otras consecuencias del delito: la responsabilidad civil ex delicto, las costas procesales y las consecuencias accesorias" en GIL GIL, Alicia, LACRUZ LÓPEZ, Juan Manuel, MELENDO PARDOS, Mariano y NÚÑEZ FERNÁNDEZ, José: *Curso de Derecho penal. Parte General*, Ed. Dykinson, Madrid, 2011.

O'REGAN, Gerard: *A brief history of computing*, Ed. Springer, 1ª edición, Londres, 2010.

OCTAVIO DE TOLEDO Y UBIETO, Emilio y HUERTA TOCILDO, Susana: *Derecho penal parte general. Teoría jurídica del delito*, Ed. Rafael Castellanos, 2ª edición, Madrid, 1986.

OCTAVIO DE TOLEDO Y UBIETO, Emilio; GURDIEL SIERRA, Manuel y CORTÉS BECHIARELLI, Emilio (coords.): *Estudios penales en recuerdo del profesor Ruiz Antón*, Ed. Tirant lo Blanch, 1ª edición, Valencia, 2004.

ORTIZ PRADILLO, Juan Carlos: "Hacking legal al servicio de la investigación criminal: nuevos instrumentos para la investigación y prueba de la delincuencia informática" en *Revista de Derecho y proceso penal*, nº 26, 2011.

ORTIZ DE URBINA GIMENO, Íñigo (coord.): *Memento Experto. Reforma Penal*, Ed. Ediciones Francis Lefebvre, 1ª edición, Madrid, 2010.

ORTS BERENGUER, Enrique y ROIG TORRES, Margarita: *Delitos informáticos y delitos cometidos a través de la informática* Ed. Tirant lo Blanch, 1ª edición, Valencia, 2001.

OVILLA BUENO, Rocío: "Algunas reflexiones jurídicas en torno al fenómeno Internet" en *Informática y derecho. Revista iberoamericana de derecho informático*, nº 27, 28 y 29, 1998.

PALOMINO MARTÍN, José María: *Derecho penal y nuevas tecnologías. Hacia un sistema informático para la aplicación del Derecho penal*, Ed. Tirant lo Blanch, 1ª edición, Valencia, 2006.

PAVÓN PÉREZ, Juan Antonio: "La labor del Consejo de Europa en la lucha contra la cibercriminalidad: El Protocolo Adicional al Convenio nº 185 sobre cibercriminalidad relativo a la incriminación de actos de naturaleza racista y xenófobos cometidos a través de los sistemas informáticos" en *Anuario de la Facultad de Derecho de la Universidad de Extremadura*, número 21, 2003.

PÉREZ ÁLVAREZ, Fernando (ed.): *Homenaje a Ruperto Núñez Barbero*, Ed. Universidad Salamanca, 1ª edición, 2007.

PÉREZ GIL, Julio: "Medidas de investigación y de aseguramiento de la prueba en el Convenio sobre el cibercrimen" en VVAA: *Libro homenaje al profesor Dr. D. Eduardo Serra Font. Tomo II*, Ed. Ministerio de Justicia, Centro de Estudios Jurídicos, 1ª edición, Madrid, 2004.

PÉREZ LUÑO, Antonio Enrique: "La protección de la intimidad frente a la informática en la Constitución española de 1978" en *Revista de Estudios Políticos*, nº 9, 1979.

PÉREZ LUÑO, Antonio Enrique: *Manual de informática y derecho*, Ed. Ariel, 1ª edición, Barcelona, 1996.

PÉREZ LUÑO, Antonio Enrique: "Internet y Derecho" en *Informática y Derecho, Jornadas marco legal y deontológico de la Informática*, nº 19-22, 1998.

PETZOLD, Charles: *The annotated Turing: a guided tour through Alan Turing's historic paper on computability and the Turing machine*, Ed. Wiley Pub, 1ª edición, Indianapolis, 2008.

PIQUERES CASTELLOTE, Francisco: "Conocimientos básicos en Internet y utilización para actividades ilícitas" en VELASCO NÚÑEZ, Eloy (dir.): *Delitos contra y a través de las nuevas tecnologías. ¿Cómo reducir su impunidad?*, Ed. Consejo General del Poder Judicial, Cuadernos de Derecho Judicial, 1ª edición, Madrid, 2006.

PICOTTI, Lorenzo: "Internet y Derecho penal: ¿un empujón únicamente tecnológico a la armonización internacional?" en ROMEO CASABONA, Carlos María (dir.): *El cibercrimen, nuevos retos jurídico-penales, nuevas respuestas político criminales*, Ed. Comares, Granada, 2006.

PRESSMAN, Rorger S.: *Ingeniería del Software, un enfoque práctico*, Ed. Mc Graw Hill, 7ª edición, Madrid, 2010.

PRIETO CAMPOS, Beatriz y PRIETO ESPINOSA, Alberto: *Conceptos de informática*, Ed. McGraw-Hill, 1ª edición, Madrid, 2005.

QUERALT JIMÉNEZ, Joan Josep: *Derecho penal español. Parte especial*, Ed. Atelier, 6ª edición, Barcelona, 2010.

QUINTERO OLIVARES, Gonzalo: *Parte General del Derecho Penal*, Ed. Thomson Reuters, 4ª edición, Navarra, 2010.

QUINTERO OLIVARES, Gonzalo: *Comentarios a la Parte Especial del Derecho Penal*, Ed. Thomson Reuters, 9ª edición, Navarra, 2011.

QUINTANO RIPOLLÉS, Antonio: *Tratado de la Parte especial de Derecho penal*, tomo III, Ed. Revista Derecho Privado, 2ª edición, Madrid, 1978.

RAGUÉS I VALLES, Ramón y ROBLES PLANAS, Ricardo: "La reforma de los delitos informáticos: incriminación de los ataques a sistemas de información" en SILVA SÁNCHEZ, Jesús María (dir.): *El nuevo código penal. Comentarios a la reforma*, Ed. La Ley, 1ª edición, Madrid, 2012.

RAYO, Agustín: "Computación cuántica" en *Investigación y Ciencia*, nº 405, 2010.

REQUEJO NAVEROS, María Teresa: *El Delito de Revelación de Secreto Médico y la Protección Penal de la Información Genética*, Ed. Colex, 1ª edición, Madrid, 2006.

REQUEJO NAVEROS, María Teresa: "Criterios de determinación de la edad penal relevante. ¿A partir de qué momento el delito cometido por un menor merece la intervención penal?" en *Crítica*, nº 976, 2011.

REYNA ALFARO, Luis Miguel: "La criminalidad informática: cuestiones para una reflexión inicial" en *Actualidad Penal*, nº 21, 2002.

RIBAS ALEJANDRO, Javier: "La sociedad digital: riesgos y oportunidades" en *Informática y derecho. Revista iberoamericana de derecho informático*, nº 27, 28 y 29, 1998.

RODRÍGUEZ BERNAL, Antonio: "España: Los Cibercrímenes en el Espacio de Libertad, Seguridad y Justicia" en *AR: Revista de Derecho Informático*, nº 103, 2007.

RODRÍGUEZ DEVESA, José María y SERRANO GÓMEZ, Alfonso: *Derecho penal español. Parte Especial*, Ed. Dykinson, 18ª edición, Madrid, 1995.

RODRÍGUEZ MOURULLO, Gonzalo; LASCURAIN SÁNCHEZ, Juan Antonio y ALONSO GALLO, Jaime: *Derecho Penal e Internet* en FERNÁNDEZ ORDÓÑEZ, Miguel Ángel; CREMADES GARCÍA, Javier e ILLESCAS ORTIZ, Rafael (coords.): *Régimen Jurídico de Internet*, Ed. La Ley, 1ª edición, Madrid, 2001.

RODRÍGUEZ MOURULLO, Gonzalo: "El Derecho penal: paradigma de la codificación", en MENÉNDEZ MENÉNDEZ, Aurelio (dir.): *La proliferación legislativa: un desafío para el Estado de Derecho*, Ed. Thomson Civitas, 1ª edición, Madrid, 2004.

RODRÍGUEZ RAMOS, Luis: "Protección penal de la propiedad industrial" en VVAA: *Propiedad Industrial teoría y práctica*, Ed. Editorial Centro de Estudios Ramón Areces, 1ª edición, Madrid, 2001.

RODRÍGUEZ RAMOS, Luis: "¿Cómo puede delinquir una persona jurídica en un sistema penal antropocéntrico? (La participación en el delito de otro por omisión imprudente: pautas para su prevención)" en *Diario La Ley*, nº 7561, 2011.

ROMEO CASABONA, Carlos María: *Poder Informático y Seguridad Jurídica*, Ed. Fundesco, 1ª edición, Madrid, 1988.

ROMEO CASABONA, Carlos María: "Delitos informáticos de carácter patrimonial" en *Informática y derecho. Revista iberoamericana de derecho informático*, nº 9, 10 y 11, 1996.

ROMEO CASABONA, Carlos María: "De los delitos informáticos al cibercrimen, una aproximación conceptual y político criminal" en ROMEO CASABONA, Carlos María (dir.): *El cibercrimen, nuevos retos jurídico-penales, nuevas respuestas político criminales*, Ed. Comares, Granada, 2006.

ROMEO CASABONA, Carlos María (dir.): *El cibercrimen, nuevos retos jurídico-penales, nuevas respuestas político criminales*, Ed. Comares, Granada, 2006.

ROMEO CASABONA, Carlos María: "De los delitos informáticos al cibercrimen" en PÉREZ ÁLVAREZ, F. (ed.): *Homenaje a Ruperto Núñez Barbero*, Ed. Universidad Salamanca, 1ª edición, 2007.

ROMEO CASABONA, Carlos María; GUANARTEME SÁNCHEZ LÁZARO, Fernando y ARMAZA ARMAZA, Emilio José (coords.): *La adaptación del Derecho penal al desarrollo tecnológico*, Ed. Comares, 1ª edición, Granada, 2010.

ROSÓN FERNÁNDEZ, Antonio: "La reforma de los delitos contra la seguridad vial. La L.O. 15/2007" en *La Ley, edición electrónica*, julio 2009.

ROVIRA DEL CANTO, Enrique: *Delincuencia informática y fraudes informáticos*, Ed. Comares, Granada, 2002.

ROXIN, Claus, edición española a cargo de LUZÓN PEÑA, Diego-Manuel; DÍAZ Y GARCÍA CONLLEDO, Miguel y DE VICENTE REMESAL, Javier: *Derecho Penal. Parte General. Tomo I*, Ed. Thomson Civitas, Navarra, 1997 (reimpresión de 2008).

RUSSELL, Deborah y GANGEMI, G. T.: *Computer Security Basics*. Ed. O'Reilly, 2ª edición, Sebastopol, 2006.

RUILOBA CASTILLA, Juan Carlos: "La actuación policial frente a los déficits de seguridad de Internet" en *Revista de Internet, derecho y política. Revista d'internet, dret i política*, nº 2, 2006.

RUIZ VADILLO, Enrique: *Tratamiento de la delincuencia informática como una de las expresiones de la criminalidad económica*, Ed. Consejo General del Poder Judicial, 1ª edición, Madrid, 1988.

RUSTAD, Michael L. y D'ANGELO, Diane: "The path of Internet law: an annotated guide to legal landmarks" en *Duke Law & Technology Review*, nº 12, 2011. (http://scholarship.law.duke.edu/cgi/viewcontent.cgi?Article=1226&context=dltr).

SALOM CLOTET, Juan: "Delito informático y su investigación" en VELASCO NÚÑEZ, Eloy (dir.): *Delitos contra y a través de las nuevas tecnologías. ¿Cómo reducir su impunidad?*, Ed. Consejo General del Poder Judicial, Cuadernos de Derecho Judicial, 1ª edición, Madrid, 2006.

SÁNCHEZ BRAVO, Álvaro A.: "La regulación de los contenidos ilícitos y nocivos en Internet" en *Informática y derecho. Revista iberoamericana de derecho informático*, nº 27, 28 y 29, 1998.

SÁNCHEZ BRAVO, Álvaro A.: "Una política comunitaria de seguridad en Internet" en *Diario La Ley*, nº 5414, 2001.

SÁNCHEZ BRAVO, Álvaro A.: "El Convenio del Consejo de Europa sobre cibercrimen: control VS. Libertades públicas" en *Diario La Ley*, nº 5528, 2002.

SÁNCHEZ GARCÍA DE PAZ, Isabel y BLANCO CORDERO, Isidoro: "Problemas de derecho penal internacional en la persecución de delitos cometidos a través de internet" en *Actualidad Penal*, nº 7, 2002.

SÁNCHEZ MEDERO, Gema: "Internet: Un espacio para el cibercrimen y el ciberterrorismo" en *Crisis analógica, futuro digital: actas del IV Congreso Online del Observatorio para la Cibersociedad, celebrado del 12 al 29 de noviembre de 2009*, Ed. Meddia, cultura i comunicación, edición electrónica, 2010.

SÁNCHEZ SISCART, José Manuel: "Cibercrimen y cooperación judicial. Especial referencia a los ISP alojados en EE.UU" en *Revista del poder judicial*, nº 91, 2011.

SÁNCHEZ-VERA GÓMEZ-TRELLES, Javier: "Sobre la figura de la autoría mediata y su tan sólo fenomenológica trascendencia" en *Anuario de derecho penal y ciencias penales*, nº 51, 1998.

SANTA CECILIA GARCÍA, Fernando.: *Delito de daños. Evolución y dogmática (art. 263 Código penal)*, Ed. Universidad Complutense de Madrid, 1ª edición, Madrid, 2003.

SCHMITT, Carl: *Die Lage der europaische Rechtswissenschaft, Internat*. Ed. Univ.-Verlag, 1ª edición, Tübingen, 1950.

SEELMANN, Kurt: "El concepto de bien jurídico, el *harm principle* y el modelo del reconocimiento como criterios de merecimiento de la pena" en HEFENDEHL, Roland: *La teoría del bien jurídico ¿Fundamento de legitimación del Derecho penal o juego de abalorios dogmáticos?*, Ed. Marcial Pons, 1ª edición, Madrid, 2007.

SIEBER, Ulrich: *The International Handbook on Computer Crime Computer-related Economic Crime and the Infringements of Privacy*, Ed. John Wiley & Sons, 1ª edición, Nueva Jersey, 1987.

SIEBER, Ulrich: "Criminalidad Informática: peligro y prevención" en MIR PUIG, S. *Delincuencia Informática*, Ed. PPU, 1ª edición, Barcelona, 1992.

SIEBER, Ulrich: "Documentación para una aproximación el delito informático" en MIR PUIG, S. *Delincuencia Informática*, Ed. PPU, 1ª edición, Barcelona, 1992.

SIEBER, Ulrich: *Information Technology Crime. National Legislations and Internationals Initiatives*, Ed. Carl Heymanns Verlag, 1ª edición, Koln, 1994.

SILVA SÁNCHEZ, Jesús María: *La expansión del derecho penal: Aspectos de la política criminal en las sociedades postindustriales*, Ed. Civitas, 2ª edición, Madrid, 2001.

SILVA SÁNCHEZ, Jesús María: "La responsabilidad penal de las personas jurídicas en el Convenio del Consejo de Europa sobre cibercriminalidad" en *Cuadernos de derecho judicial*, nº 9, 2002.

SILVA SÁNCHEZ, Jesús María (dir.): *El nuevo código penal. Comentarios a la reforma*, Ed. La Ley, 1ª edición, Madrid, 2012.

SKIBELL, Reid: "Cybercrimes & misdemeanors: a reevaluation of the Computer Fraud and Abuse Act" en *Berkeley Technology Law Journal*, nº 18, 2003.

SMITH, Michael T.: *Station X: The Codebreakers of Bletchley Park, Pan Grand Strategy Series*, Ed. Pan McMillan Ltd, 1ª edición revisada, Londres, 2007.

SNEYERS PODOLSKY, Alfredo: *El fraude y otros delitos informáticos*, Ed. Tecnologías de Gerencia y Producción, 1ª edición, Madrid, 1990.

SOMMERVILLE, Ian: *Ingeniería del software*, Ed. Pearson Educación, 7ª edición, Madrid, 2005.

STOKES, Jon M.: *Inside the Machine: An Illustrated Introduction to Microprocessors and Computer Architecture*, Ed. No Starch Press, 1ª edición, San Francisco, 2006.

STRATENWERTH, Günter: "La criminalización en los delitos contra bienes jurídicos colectivos" en HEFENDEHL, Roland: *La teoría del bien jurídico ¿Fundamento de legitimación del Derecho penal o juego de abalorios dogmáticos?*, Ed. Marcial Pons, 1ª edición, Madrid, 2007.

SUÑÉ LLINÁS, Emilio: *Tratado de Derecho Informático Volumen I*, Ed. Complutense, 1ª edición, Madrid, 2002.

TANENBAUM, Andrew S.: *Redes de computadoras*, Ed. Pearson Educación, 4ª edición, Madrid, 2003.

TÉLLEZ VALDEZ, Julio: D*erecho informático*. Ed. Mc Graw Hill, 2ª edición, México, 1996.

TÉLLEZ VALDÉS, Julio: "Delitos cibernéticos" en *Informática y derecho. Revista iberoamericana de derecho informático*, nº 27, 28 y 29, 1998.

TEUBNER, Gunther: "Globalización y constitucionalismo social: alternativas a la teoría constitucional centrada en el Estado" en BACIGALUPO SAGGESE, Silvina y CANCIO MELIÁ, Manuel (coords.): *Derecho penal y política transnacional*, Ed. Atelier, 1ª edición, Barcelona, 2005.

URBANO CASTRILLO, Eduardo: "Infracciones patrimoniales por medios informáticos y contra la información, como bien económico" en VELASCO NÚÑEZ, Eloy (dir.): *Delitos contra y a través de las nuevas tecnologías. ¿Cómo reducir su impunidad?*, Ed. Consejo General del Poder Judicial, Cuadernos de Derecho Judicial, 1ª edición, Madrid, 2006.

URBANO CASTRILLO, Eduardo: "Los delitos informáticos tras la reforma del CP de 2010" en *Revista Aranzadi Doctrinal*, nº 9, 2010.

URBANO CASTRILLO, Eduardo: "Los delitos informáticos tras la reforma del CP de 2010" en *Delincuencia informática. Tiempos de cautela y amparo*, Ed. Thomson Reuters Aranzadi, 1ª edición, Navarra, 2012.

VANDELLI, Luciano: *Trastornos de las instituciones políticas*, Ed. Trotta, 1ª edición, Madrid, 2007.

VÁZQUEZ IRUZUBIETA, Carlos: *Manual de Derecho Informático*, Ed. Dijusa, 1ª edición, Madrid, 2002.

VELASCO NÚÑEZ, Eloy: "Cuestiones procesales relativas a la investigación de los delitos informáticos" en VELASCO NÚÑEZ, Eloy (dir.): *Delitos contra y a través de las nuevas tecnologías. ¿Cómo reducir su impunidad?*, Ed. Consejo General del Poder Judicial, Cuadernos de Derecho Judicial, 1ª edición, Madrid, 2006.

VELASCO NÚÑEZ, Eloy (dir.): *Delitos contra y a través de las nuevas tecnologías. ¿Cómo reducir su impunidad?*, Ed. Consejo General del Poder Judicial, Cuadernos de Derecho Judicial, 1ª edición, Madrid, 2006.

VELASCO NÚÑEZ, Eloy: "Aspectos procesales de la investigación y de la defensa en los delitos informáticos" en *Diario La Ley*, nº 6506, 2006.

VELASCO NÚÑEZ, Eloy: *Delitos cometidos a través de Internet. Cuestiones procesales*, Ed. La Ley, 1ª edición, Madrid, 2010.

VELASCO NÚÑEZ, Eloy: "La investigación de delitos informáticos con garantías judiciales: nuevos formatos para la delincuencia" en *Telos: Cuadernos de comunicación e innovación*, nº 85, 2010.

VELASCO NÚÑEZ, Eloy: "Delitos informáticos realizados en actuación organizada" en *Diario La Ley*, nº 7743, 2011.

VELASCO SAN MARTÍN, Cristos: *La jurisdicción y competencia sobre delitos cometidos a través de sistema de cómputo e internet*, Ed. Tirant lo Blanch, 1ª edición, Valencia, 2012.

VILLÉN SOTOMAYOR, Marta: "La red y su evolución y utilización para actividades ilícitas" en VELASCO NÚÑEZ, Eloy (dir.): *Delitos contra y a través de las nuevas tecnologías. ¿Cómo reducir su impunidad?*, Ed. Consejo General del Poder Judicial, Cuadernos de Derecho Judicial, 1ª edición, Madrid, 2006.

VV.AA.: *The Melissa virus : inoculating our information technology from emerging threats : hearing before the Committee on Science, Subcommittee on Technology, U.S. House of Representatives, One Hundred Sixth Congress, first session, April 15, 1999*, Ed. U.S. Government Printing Office, 1ª edición, Washington DC, 1999

VV.AA.: *Propiedad Industrial teoría y práctica*, Ed. Editorial Centro de Estudios Ramón Areces, 1ª edición, Madrid, 2001.

VV.AA.: *Libro homenaje al profesor Dr. D. Eduardo Serra Font. Tomo II*, Ed. Ministerio de Justicia, Centro de Estudios Jurídicos, 1ª edición, Madrid, 2004.

VV.AA.: *Delincuencia informática. Tiempos de cautela y amparo*, Ed. Thomson Reuters Aranzadi, 1ª edición, Navarra, 2012.

WALL, David S.: *Cybercrime. The transformation of crime in the information age*, Ed. Polity Press, 1ª edición, Cambridge, 2007.

WELCHMAN, Gordon: *The Hut Six story: Breaking the Enigma codes*, Ed. Penguin Books, 1ª edición revisada, Harmondsworth, 1984.

WOHLERS, Wolfgang: "Las jornadas desde la perspectiva de un escéptico del bien jurídico" en HEFENDEHL, Roland: *La teoría del bien jurídico ¿Fundamento de legitimación del Derecho penal o juego de abalorios dogmáticos?*, Ed. Marcial Pons, 1ª edición, Madrid, 2007.

YAR, Majid: *Cybercrime and society*, Ed. Sage, 1ª edición, Londres, 2006.

ZORRAQUINO RICO, Assumpta: "Delitos informáticos" en *Cuadernos de derecho judicial*, nº 5, 2006.

ZUGALDÍA ESPINAR, José Miguel: "Los delitos contra la propiedad, el patrimonio y el orden socioeconómico en el nuevo Código Penal (consideraciones generales sobre el Título XIII del N.C.P)" en *Cuadernos de política criminal*, nº 59, 1996.

ZUGALDÍA ESPINAR, José Miguel: "¿Qué queda en pie en el Derecho penal del principio de mínima intervención, máximas garantías?" en *Cuadernos de política criminal*, nº 79, 2003.

ZUGALDÍA ESPINAR, José Miguel: "Terrorismo y globalización" en LÓPEZ CALERA, Nicolás María (coord.): La palabra contra el terrorismo, Ed. Universidad de Granada, 1ª edición, Granada, 2004.

ZUGALDÍA ESPINAR, José Miguel: "Seguridad ciudadana y Estado social de Derecho (A propósito del Código penal de la Seguridad y el pensamiento funcionalista)" en OCTAVIO DE TOLEDO Y UBIETO, Emilio; GURDIEL SIERRA, Manuel y CORTÉS BECHIARELLI, Emilio (coords.): *Estudios penales en recuerdo del profesor Ruiz Antón*, Ed. Tirant lo Blanch, 1ª edición, Valencia, 2004.

ZUGALDÍA ESPINAR, José Miguel: *Fundamentos de derecho penal*, Ed. Tirant lo Blanch, 4ª edición, Valencia, 2010.

ZUGALDÍA ESPINAR, José Miguel: *La responsabilidad criminal de las personas jurídicas, de los entes sin personalidad y de sus directivos*, Ed. Tirant lo Blanch, 1ª edición, Valencia, 2013.

Otras fuentes:

AIDP: "Computer Crime and Other Crimes Aganits Informátion Technology" en *Internacional Review of Penal Law*, Ed. Erès, nº 64, 1º y 2º trimestres, 1993.

Anonymus: http://www.anonops.net/

Artículo -sin firma- "*Programmer Convicted After Planting a Virus*" publicado en el *NY Times* el 21 de septiembre de 1988.

Artículo -sin firma- "*Mad boffin jailed over computer virus havoc*" publicado en *The Independent* el 16 de noviembre de 1995.

Artículo -sin firma- "Nueva estrategia comunitaria contra el cibercrimen: La Comisión europea presenta una comunicación" en *Europa Euskadi*, nº 220, 2007.

Artículo -sin firma- "¿Qué es la ciberdelincuencia?" en *Cuadernos de criminología: revista de criminología y ciencias forenses*, nº 9, 2010.

Centre for Quantum Computation: http://www.qubit.org

CNI, página web del CERT: https://www.ccn-cert.cni.es/

Departamento de matemática aplicada de la Universidad Politécnica de Madrid: http://www.eui.upm.es/escuela/dptos/ma

Donald Gene Burleson, appellant v. The State of Texas, State nº 2-88-301-CR. Court of appeals of Texas, Second District, Fort Worth 802 S.W.2d 429; 1991 Tex. App. LEXIS 229. January 25, 1991.

EISAS: *European Information Sharing and Alert System. A Feasibility Study 2006/2007*: http://www.enisa.europa.eu/activities/cert/other-work/eisas_folder/EISAS_finalreport.pdf

European Public-Private Partnership for Resilience, sus objetivos, principios y estructura se describen en el documento sobre el establecimiento de la EP3R elaborado en junio de 2010: http://ec.europa.eu/information_society/policy/nis/docs/ep3r_workshops/3rd_june2010/2010_06_23_ep3r_nonpaper_v_2_0_final.pdf

Grupo de Investigación en Información y Computación Cuántica de la Universidad Politécnica de Madrid: http://gcc.ls.fi.upm.es

Informe Microsoft sobre *software malicioso en* 2012: http://www.microsoft.com/security/sir/story/#!10year

Institute for Quantum Computing: http://iqc.uwaterloo.ca

Instrucción 2/2011, sobre el fiscal de sala de criminalidad informática y las secciones de criminalidad informática de las fiscalías.

INTECO, página web: http://cert.inteco.es

INTECO, redes *Zombie:* http://cert.inteco.es/Formacion/Amenazas/botnets/

Memoria 2010 de la Fiscalía General del Estado de España.

Memoria 2011 de la Fiscalía General del Estado de España.

Memoria 2012 de la Fiscalía General del Estado de España.

National Museum of American History, objeto 1994.0191.01: http://americanhistory.si.edu/collections

OCDE, página web: http://http://www.oecd.org/about/

OCDE: "Computer-related crime: analysis of legal policy" en ICCP - *Information, computer and communications policy*, Ed. OECD Publications and Information Centre, nº 10, Washington, 31 de agosto de 1986.

OCDE: "Guidelines for the Security of Information Systems", 1992: www.oecd.org/internet/interneteconomy/oecdguidelinesforthesecurityofinformationsystems1992.htm

OCDE: "Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security", 2002: http://www.oecd.org/internet/interneteconomy/34912912.pdf

ONU, página web: http://www.un.org/es/aboutun/

ONU: Informe general del 8º Congreso de las Naciones Unidas sobre Prevención del Delito y Justicia Penal, La Habana, Cuba, 27 de agosto a 7 de septiembre de 1990.

ONU: Informe general del 9º Congreso de las Naciones Unidas sobre Prevención del Delito y Justicia Penal, El Cairo, Egipto, 29 de abril a 8 de mayo de 1995.

ONU: Informe general del 10º Congreso de las Naciones Unidas sobre Prevención del Delito y Justicia Penal, Viena, Austria, 10 a 17 de abril de 2000.

ONU: Informe A/CONF.187/10 del 10º Congreso de las Naciones Unidas sobre Prevención del Delito y Justicia Penal, Viena, Austria, 10 a 17 de abril de 2000.

ONU: Informe general del 11º Congreso de las Naciones Unidas sobre Prevención del Delito y Justicia Penal, Bangkok, Tailandia, 18 a 25 de abril de 2005.

ONU: Informe general del 12º Congreso de las Naciones Unidas sobre Prevención del Delito y Justicia Penal, Salvador, Brasil, 12 a 19 de abril de 2010.

ONU: "Manual de las Naciones Unidas sobre prevención y control de delitos informáticos" en *Revista Internacional de Política Criminal*, Ed. Naciones Unidas, nº 43 y 44, 1994. El texto completo: http://www.uncjin.org/documents/irpc4344.pdf

ONU: "Manual de las Naciones Unidas sobre prevención y control de delitos informáticos" en *Revista Internacional de Política Criminal*, Ed. Naciones Unidas, nº 43 y 44, 1994.

Recommendation nº R(89)9 of the Committee of Ministers to Member States on Computer-related Crime and Final Report of the European Committe on Crime Problems (aprobada por el Comité de Ministros el 13 de septiembre 1989 en la reunión 428 de Delegados), Ed. Council of Europe Publishing and Documentation Service, Estrasburgo, 1990.

Recommendation nº R(95)13 of the Committee of Ministers to Member States Concerning Problems of Criminal Procedural Law Connected with Information Technology (aprobada por el Comité de Ministros el 11 de septiembre 1995 en la reunión 543 de Delegados), Ed. Council of Europe Publishing and Documentation Service, Estrasburgo, 1995.

S.M.H COLLIN: *Dictionary of computing*, Ed. Blomsbury Publishing, 5ª edición, Londres, 2004.

United States v. Morris, 928 F.2d 504, 505 (2d Cir. 1991).

United States v. David Smith, Case Number 2:99-CR-730-01 (US District Court of New Jersey, 1999).

WEF: *Global Risk 2008,* Ed. World Economic Forum, 1ª edición, Ginebra, 2008.

ÍNDICE DE LEGISLACIÓN

Normativa española:

Constitución Española de 1978.

Ley Orgánica 5/2010, de 22 de junio, por la que se modifica la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal.

Ley Orgánica 5/2000, de 12 de enero, reguladora de la responsabilidad penal de Ley Orgánicas menores.

Ley Orgánica 15/1999 de 13 de diciembre, de Protección de Datos de Carácter Personal.

Ley Orgánica 11/1999, de 30 de abril, de reforma del Código penal.

Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal.

Ley Orgánica 1/1992, de 21 de febrero, sobre Protección de la Seguridad Ciudadana.

Ley Orgánica 2/1986, de 13 de marzo, de Fuerzas y Cuerpos de Seguridad del Estado.

Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial.

Ley Orgánica 7/1984 de 15 de octubre, sobre tipificación penal de colocación ilegal de escuchas telefónicas.

Ley Orgánica 8/1983 de 25 de junio, de reforma urgente y parcial del Código Penal.

Ley Orgánica 2/1981 de 4 de mayo, por la que se modifica el delito de rebelión y el de asociación ilícita.

Ley Orgánica 3/1980, de 22 de abril, del Consejo de Estado.

Ley 2/2011, de 4 de marzo, de Economía Sostenible.

Ley 50/1997, de 27 de noviembre, del Gobierno.

Real Decreto 400/2012, de 17 de febrero, por el que se desarrolla la estructura orgánica básica del Ministerio del Interior.

Real Decreto 1083/2009, de 3 de julio, por el que se regula la memoria del análisis de impacto normativo.

Real Decreto 160/1997, de 7 de febrero, por el que se aprueban los Estatutos de la Comisión General de Codificación.

Real Decreto Legislativo 1/1996, de 12 de abril, por el que se aprueba el texto refundido de la Ley de Propiedad Intelectual, regularizando, aclarando y armonizando las disposiciones legales vigentes sobre la materia.

Orden del Ministerio de Justicia de 8 de abril de 2005, sobre la creación de una Sección Especial para la Revisión del Código Penal en el seno de la Comisión General de Codificación.

Normativa comunitaria:

Tratado de Lisboa, de 13 de diciembre de 2007.

Tratado de Ámsterdam, de 2 de octubre de 1997.

Tratado de la Unión Europa, de 7 de febrero de 1992.

Tratado del Acta Única Europea, de 17 y 28 de febrero de 1986.

Tratado de Groenlandia, de 13 de marzo de 1984.

Tratado que modifica algunas disposiciones financieras, de 22 de julio de 1975.

Tratado de Fusión por el que se constituye un Consejo único y una Comisión única de las Comunidades Europeas, de 8 de abril de 1965.

Tratado Constitutivo de la Comunidad Económica Europea, de 25 de marzo de 1957.

Directiva 2011/93/UE del Parlamento Europeo y del Consejo, de 13 de diciembre de 2011, relativa a la lucha contra los abusos sexuales y la explotación sexual de los menores y la pornografía infantil.

Directiva 2008/114/CE del Consejo, de 8 de diciembre de 2008, sobre la identificación y designación de infraestructuras críticas europeas y la evaluación de la necesidad de mejorar su protección.

Decisión Marco 2005/222/JAI del Consejo, de 24 de febrero de 2005, relativa a los ataques contra los sistemas de información.

Decisión Marco 2004/68/JAI del Consejo, de 22 de diciembre de 2003, relativa a la lucha contra la explotación sexual de los niños y la pornografía infantil.

Decisión Marco 2001/413/JAI del Consejo, de 28 de mayo de 2001, sobre la lucha contra el fraude y la falsificación de medios de pago distintos del efectivo.

Decisión 91/242/CEE del Consejo, de 31 de marzo de 1992, relativa a la seguridad de los sistemas de información.

Reglamento (CE) n° 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.

Acción Común 98/733/JAI, de 21 de diciembre de 1998, adoptada por el Consejo sobre la base del artículo K.3 del Tratado de la Unión Europea, relativa a la tipificación penal de la participación en una organización delictiva en los Estados miembros de la Unión Europea.

Acción común 97/154/JAI, de 24 de febrero de 1997, adoptada por el Consejo sobre la base del artículo K.3 del Tratado de la Unión Europea, relativa a la lucha contra la trata de seres humanos y la explotación sexual de los niños COM(2000) 890 final, de 26 de enero de 2001.

Comunicación COM(2012) 140 final, de 28 de marzo de 2012. Comunicación de la Comisión al Consejo y al Parlamento Europeo: La represión del delito en la era digital, creación de un centro europeo de Ciberdelincuencia

Comunicación COM(2011) 163 final, de 31 de marzo de 2001. Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones sobre la protección de infraestructuras críticas de información: logros y próximas etapas: hacia la ciberseguridad global.

Comunicación COM(2010) 517 final, de 30 de septiembre de 2010. Propuesta de Directiva del Parlamento Europeo y del Consejo Relativa a los ataques contra los sistemas de información, por la que se deroga la Decisión marco 2005/222/JAI del Consejo.

Comunicación COM(2009) 149 final, de 30 de marzo de 2009. Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones sobre protección de infraestructuras críticas de información: Proteger Europa de ciberataques e interrupciones a gran escala: aumentar la preparación, seguridad y resistencia.

Comunicación COM(2008) 448 final, de 14 de julio de 2008. Informe de la Comisión al Consejo basado en el artículo 12 de la Decisión Marco del Consejo, de 24 de febrero de 2005, relativa a los ataques contra los sistemas de información.

Comunicación COM(2007) 716 final, de 16 de noviembre de 2007. Informe de la Comisión basado en el artículo 12 de la Decisión Marco 2004/68/JAI del Consejo, de 22 de diciembre de 2003, relativa a la lucha contra la explotación sexual de los niños y la pornografía infantil.

Comunicación COM(2007) 267 final, de 22 de mayo de 2007. Comunicación de la Comisión al Parlamento Europeo, al Consejo y al Comité de las Regiones: hacia una política general de lucha contra la ciberdelincuencia.

Comunicación COM(2001) 298 final, 6 de junio de 2001. Comunicación de la Comisión al Consejo, al Parlamento Europeo, al Comité Económico y Social y al Comité de las Regiones: seguridad de las redes y de la información: Propuesta para un enfoque político europeo.

Normativa internacional:

Convenio 185 del Consejo de Europa sobre la Ciberdelincuencia celebrado en Budapest el 23 de noviembre de 2001.

Convenio 108 del Consejo de Europa para la Protección de las Personas con respecto al Tratamiento Automatizado de Datos de Carácter Personal celebrado en Estrasburgo el 28 de enero de 1981.

Convenio Europeo de Asistencia Judicial en Materia Penal de 20 de abril de 1959.

Convenio Europeo para la Protección de los Derechos Humanos y las Libertades Fundamentales de 4 de noviembre de 1950.

Protocolo adicional al Convenio 185 del Consejo de Europa sobre la Ciberdelincuencia relativo a la incriminación de actos de naturaleza racista y xenófobos cometidos a través de los sistemas informáticos de 2003.

Pacto Internacional de Derechos Civiles y Políticos de las Naciones Unidas de 16 de diciembre de 1966.

Declaración Universal de Derechos Humanos de 10 de diciembre de 1948.

Otras normativas:

EEUU: Counterfeit Access Device and Abuse Act de 1984 [Referencia legal Pub. L. Nº 98-473].

EEUU: Computer Fraud and Abuse Act de 1986 [Referencia legal Pub. L. Nº 99-474].

EEUU: Economic Espionage Act de 1996 [Referencia legal Pub. L. Nº 104-294].

EEUU: USA Patriot Act1 de 2001 [Referencia legal Pub. L. Nº 107-56].

Alemania: Zweites Gesetz zur Bekampfung der Wirtschaftskriminalitat (2.wikg) o Segunda Ley para la lucha contra la criminalidad económica, de 15 de mayo de 1986.

Austria: Ley de reforma del Código penal de 22 de diciembre de 1987.

Francia: Loi nº 88-19 du 5 janvier 1988 relative à la fraude informatique o Ley 88-19 de 5 de enero de 1988 sobre el fraude informático.

Reino Unido: Computer Misuse Act de 1990.

Italia: Ley de reforma del Código penal de 1993.

Italia: Ley de reforma del Código penal de 1995.

ÍNDICE DE JURISPRUDENCIA

Tribunal Europeo de Derechos Humanos:

P. G. y J. H. contra Reino Unido, Sentencia de la sección 3ª, de 25 de septiembre de 2001.

Tribunal de Justicia de las Comunidades Europeas:

Sentencia del Tribunal de Justicia de las Comunidades Europeas, de 21 de septiembre 1989.

Tribunal Constitucional:

Sentencia 64/2001, de 17 de marzo.
Sentencia 120/1999, de 27 de junio.
Sentencia 30/1999, de 8 de marzo.
Sentencia 11/1998, de 13 de enero.
Sentencia 86/1996, de 21 de mayo.
Sentencia 325/1994, de 12 de diciembre.
Sentencia 71/1994, de 3 de marzo.
Sentencia 372/1993, de 13 de diciembre.
Sentencia 111/1993, de 25 de marzo.
Sentencia 104/1989, de 8 de junio.
Sentencia 133/1987, de 21 de julio.
Sentencia 59/1985, de 6 de mayo.
Sentencia 123/1984, de 18 de diciembre.
Sentencia 117/1984, de 5 de diciembre.
Sentencia 62/1982, de 15 de octubre.
Sentencia 33/1982, de 8 de junio.

Tribunal Supremo:

Sentencia 1387/2011, de 12 diciembre.
Sentencia 588/2010, de 22 de junio.
Auto de 17 de marzo 2009.
Sentencia 1030/2007, de 4 de diciembre.
Sentencia 1136/2006, de 21 de diciembre.
Sentencia 913/2006, de 20 de septiembre.
Sentencia 1093/2006, de 18 de octubre.
Sentencia 37/2006, de 25 de enero.
Sentencia 1444/2004, de 10 de diciembre.
Sentencia 334/2003, de 5 de marzo.
Sentencia 2392/2001, de 10 de diciembre.

Sentencia 1479/2000, de 22 de septiembre.

Sentencia 88/1999, de 27 de enero.

Sentencia de 27 de abril de 1992.

Sentencia de 27 de junio de 1991.

Sentencia de 19 de abril de 1991.

Sentencia de 13 de diciembre de 1990.

Sentencia de 27 de mayo de 1988

Sentencia de 5 de febrero de 1988.

Sentencia 2 de Noviembre de 1987, Sala de lo Contencioso-Administrativo.

Sentencia de 29 de noviembre de 1984.

Sentencia de 30 de noviembre de 1981.

Sentencia de 5 de abril de 1966.

Jurisprudencia menor:

Sentencia de la AN 5/2012, de 6 de febrero.

Sentencia de la AP de Barcelona 72/2008, de 18 enero.

Sentencia del Juzgado de lo penal 2 de Lleida 33/2006, de 7 de febrero.

Sentencia del Juzgado de lo penal 1 de Terrassa 20/2006, de 1 febrero.

Auto de la AP de Madrid 229/2004, de 21 de mayo.

Auto del Juzgado de instrucción 2 de Lorca de 29 de enero de 2002.

Sentencia de la AP de Tarragona, de 23 de julio de 2001.

Auto de la AP de Barcelona 326/2000, de 30 de octubre.

Sentencia del Juzgado de lo penal 2 de Barcelona, de 28 de mayo de 1999.