PROGRAMA DE DOCTORADO

"Estudios Jurídicos, Ciencia Política y Criminología"

# EL DELITO DE *HACKING*

TOMO I

TESIS DOCTORAL

Autor: Francisco Almenar Pineda

Directora: Dra. Paz Lloria García

Departamento de Derecho penal

Facultad de Derecho de la Universidad de Valencia

Valencia, mayo de 2017

Certificado de dirección de la tesis.

Dra. Paz Lloria García

Agradecimientos:

A Paz.

A mis padres, Paco y Coro.

A Miguel Soler.

**ÍNDICE GENERAL**

**TOMO I**

ABREVIATURAS ..... 17

INTRODUCCIÓN ..... 21

CAPÍTULO I. ANTECEDENTES Y EVOLUCIÓN DEL *HACKING* ..... 31

1. INTRODUCCIÓN ..... 33
   - 1.1 El nacimiento de la red y su vinculación con la intimidad..... 33
   - 1.2 El concepto de Derecho penal informático ..... 40
   - 1.3 Rasgos de la delincuencia informática ..... 49
2. EVOLUCIÓN HISTÓRICA ..... 53
   - 2.1 Las primeras manifestaciones ..... 53
   - 2.2 La expansión del uso de Internet ..... 64
   - 2.3 Evolución normativa en el ámbito supranacional ..... 68
3. CONCEPTO DE *HACKING* ..... 80
   - 3.1 El concepto sociológico y gramatical ..... 80
   - 3.2 El concepto normativo ..... 85
4. EL *HACKING* EN EL ORDENAMIENTO PENAL ESPAÑOL ..... 90
   - 4.1 La situación antes de la reforma de 2010 ..... 90
   - 4.2 La justificación de las reformas de los años 2010 y 2015 ..... 105
     - 4.2.1 La reforma del año 2010 ..... 105

4.2.1.1 El Convenio Europeo sobre Cibercriminalidad ..... 107
4.2.1.2 La DM 2005/222/JAI ..... 111
4.2.2 La reforma del año 2015 y la Directiva 2013/40/UE ..... 114
4.3 La tramitación parlamentaria de las reformas de los años 2010 y 2015 ..... 125
4.3.1 La reforma del año 2010 ..... 125
4.3.2 La reforma del año 2015 ..... 145

CAPÍTULO II. BREVE REFERENCIA AL DELITO DE *HACKING* EN EL DERECHO COMPARADO EUROPEO ..... 159

1. INTRODUCCIÓN ..... 161
2. PAÍSES QUE REGULAN LOS DELITOS INFORMÁTICOS EN NORMAS PENALES ESPECIALES.....163
   2.1 Chipre ..... 163
   2.2 Portugal ..... 167
   2.3 Reino Unido ..... 171
3. PAÍSES QUE REGULAN EL DELITO DE *HACKING* EN UN TÍTULO O CAPÍTULO PROPIO Y DIFERENCIADO ..... 178
   3.1 Bélgica ..... 179

3.2 Bulgaria ..... 184
3.3 Croacia ..... 187
3.4 Finlandia ..... 193
3.5 Hungría ..... 197
4. PAÍSES QUE REGULAN EL DELITO DE *HACKING* JUNTO A OTROS DELITOS ..... 203
4.1 Alemania ..... 203
4.2 Austria ..... 207
4.3 Dinamarca ..... 210
4.4 Eslovaquia ..... 214
4.5 Eslovenia ..... 218
4.6 Estonia ..... 220
4.7 Francia ..... 222
4.8 Grecia ..... 227
4.9 Holanda ..... 229
4.10 Irlanda ..... 232
4.11 Italia ..... 238
4.12 Letonia ..... 242
4.13 Lituania ..... 245
4.14 Luxemburgo ..... 248
4.15 Malta ..... 252
4.16 Polonia ..... 257
4.17 República Checa ..... 259
4.18 Rumania ..... 265
4.19 Suecia ..... 268
5. CONCLUSIONES ..... 270

CAPITULO III. BIEN JURÍDICO PROTEGIDO Y OBJETO MATERIAL EN EL DELITO DE *HACKING* ..... 273

1. INTRODUCCIÓN ..... 275
2. PLANTEAMIENTO ..... 278
3. EL DELITO DE *HACKING* COMO DELITO CONTRA LA INTIMIDAD ..... 284
   - 3.1 Introducción ..... 284
   - 3.2 Aproximación al bien jurídico protegido común de los delitos contra la intimidad ..... 286
     - 3.2.1 Evolución histórica ..... 289
     - 3.2.2 Intimidad, secreto, *habeas data* y propia imagen ..... 302
   - 3.3 El *hacking* como delito contra la intimidad ..... 307
   - 3.4 Críticas a la consideración del delito de *hacking* como un delito contra la intimidad ..... 309
   - 3.5 La seguridad de los sistemas informáticos como bien jurídico protegido ..... 317
4. EL OBJETO MATERIAL ..... 331
   - 4.1 El objeto material en la regulación tras la LO 5/2010 ..... 332
   - 4.2 El objeto material en la regulación tras la LO 1/2015 ..... 334
5. NATURALEZA JURÍDICA DEL DELITO DE *HACKING* ..... 341
6. TOMA DE POSICIÓN ..... 356

**TOMO II**

CAPÍTULO IV. EL DELITO DE *HACKING* ..... 379

1. INTRODUCCIÓN ..... 381
2. EL ARTÍCULO 197 *BIS* 1 CP ..... 388
   - 2.1 Los sujetos ..... 391
     - 2.1.1 Sujeto activo ..... 393
     - 2.1.2 Sujeto pasivo ..... 394
   - 2.2 La conducta típica ..... 396
     - 2.2.1 El verbo típico: "acceder a un sistema de información" ..... 400
     - 2.2.2 La exigencia de "medidas de seguridad establecidas para impedirlo" ..... 410
     - 2.2.3 El concepto de no "estar debidamente autorizado"..... 417
     - 2.2.4 Los elementos delimitadores de facilitar el *hacking* en el artículo 197 *bis* 1 en relación con las conductas del nuevo artículo 197 *ter* ..... 436
     - 2.2.5 Los elementos delimitadores del *hacking* en relación con la conducta de mantenimiento en el sistema de información (artículo 197 *bis* 1) . 445
3. POSICIÓN PERSONAL ..... 453
   - 3.1 Planteamiento ..... 453
   - 3.2 Respecto al elemento de acceder a un sistema de información ..... 459

3.3 Las medidas de seguridad establecidas para impedirlo ..... 461

3.4 No estar debidamente autorizado ..... 462

3.5 Elementos delimitadores de facilitar el *hacking* en el artículo 197 *bis* 1 en relación con las conductas del nuevo artículo 197 *ter* ..... 464

3.6 Elementos delimitadores del *hacking* en relación con la conducta de mantenimiento en el sistema de información ..... 468

4. ASPECTO SUBJETIVO ..... 472

5. FORMAS DE APARICIÓN ..... 476

5.1 Autoría y participación ..... 477

5.1.1 Autoría ..... 480

5.1.2 Participación ..... 485

5.2 *Iter Criminis* ..... 492

5.2.1 Actos preparatorios ..... 494

5.2.2 Tentativa ..... 496

5.2.3 Consumación ..... 507

5.3 Relaciones concursales ..... 509

5.3.1 El *hacking* del artículo 197 *bis* 1 y la conducta del artículo 197 *ter* ..... 510

5.3.2 El *hacking* del artículo 197 *bis* 1 y el allanamiento de morada de los artículos 202.1 y 203.1 ..... 512

5.3.3 El *hacking* del artículo 197 *bis* 1 y las conductas del artículo 197.2 ..... 514

5.3.4 El *hacking* del artículo 197 *bis* 1 y las conductas del artículo 264..... 516

5.3.5 El *hacking* del artículo 197 *bis* 1 y otros delitos ..... 517

6. TOMA DE POSICIÓN ..... 522

6.1 Aspecto subjetivo ..... 522

6.2 Autoría y participación ..... 524

6.3 *Iter criminis* ..... 529

6.4 Relaciones concursales ..... 535

CAPÍTULO V. LOS TIPOS AGRAVADOS DEL *HACKING* ..... 541

1. INTRODUCCIÓN ..... 543
2. EL TIPO AGRAVADO DEL ARTÍCULO 197 *QUATER* . 550

2.1 Fundamento del tipo agravado ..... 550

2.2 La conducta del artículo 197 *quater* ..... 561

2.3 Posición personal ..... 576

3. EL TIPO AGRAVADO DEL ARTÍCULO 198 ..... 583

3.1 El concepto de "autoridad o funcionario público" .. 587
3.2 La actuación "fuera de los casos permitidos por la Ley"..... 593
3.3 La actuación "sin mediar causa legal por delito" ..... 600
3.4 La actuación "prevaliéndose de su cargo" ..... 602
3.5 Punto de vista personal ..... 607

CAPÍTULO VI. RESPONSABILIDAD PENAL DE LAS PERSONAS JURÍDICAS EN EL DELITO DE *HACKING* ..... 617

1. INTRODUCCIÓN ..... 619
2. RESPONSABILIDAD PENAL DE LA PERSONA JURÍDICA EN EL DELITO DE *HACKING* ..... 628
   2.1 Planteamiento ..... 628
   2.2 Aproximación al concepto de persona jurídica en el delito de *hacking* ..... 633
   2.3 Las conductas llevadas a cabo por sus representantes legales o por quienes están sometidos a su autoridad .. 647
   2.4 La exigencia de responsabilidad penal a la persona jurídica por el delito de *hacking*..... 658
3. TOMA DE POSICIÓN ..... 671

CONCLUSIONES ..... 679

ÍNDICE DE DOCUMENTOS ..... 719

JURISPRUDENCIA CONSULTADA ..... 749

BIBLIOGRAFÍA CONSULTADA ..... 761

## ABREVIATURAS

| | |
|---|---|
| AAP | Auto de la Audiencia Provincial |
| ADPCP | Anuario de Derecho penal y Ciencias penales |
| AJA | Actualidad Jurídica Aranzadi |
| BOCG | Boletín Oficial de las Cortes Generales |
| BOE | Boletín Oficial del Estado |
| CE | Constitución Española de 1978 |
| CEDH | Convenio Europeo para la protección de los Derechos Humanos y las Libertades Fundamentales, del 4 de noviembre de 1950 |
| CGPJ | Consejo General del Poder Judicial |
| CP | Ley Orgánica 10/1995, de 23 de noviembre, por la que se aprueba el Código Penal |
| DM | Decisión Marco |
| DOUE | Diario Oficial de la Unión Europea |
| DUDH | Declaración Universal de los Derechos Humanos, adoptada y proclamada por la 183ª Asamblea General de la Organización de Naciones Unidas en París el 10 de Diciembre de 1948 |
| EDJ | Base de Datos El Derecho Jurisprudencia |

| | |
|---|---|
| FGE | Fiscalía General del Estado |
| FJ | Fundamento Jurídico |
| ICT | "*Information and Communications Technology*" |
| LO | Ley Orgánica |
| LOPD | Ley Orgánica de Protección de Datos |
| LPI | Ley de Propiedad Intelectual |
| PIDCP | Pacto Internacional de Derechos Civiles y Políticos |
| Pte. | Ponente |
| RAE | Real Academia Española |
| RAP | Revista de Administración Pública |
| RGDP | Revista General de Derecho Penal |
| RJ | Repertorio de Jurisprudencia Aranzadi |
| RTC | Repertorio Aranzadi del Tribunal Constitucional |
| SAN | Sentencia de la Audiencia Nacional |
| SAP | Sentencia de la Audiencia Provincial |
| STC | Sentencia del Tribunal Constitucional |
| STS | Sentencia del Tribunal Supremo |
| TIC | Tecnologías de la Información y la Comunicación |
| VVAA | Varios Autores |

## INTRODUCCIÓN

El objeto de estudio del trabajo se centra en la conducta de acceso ilícito a los sistemas informáticos y constituye un claro ejemplo de la necesidad de adaptar el Derecho a los cambios que surgen en la vida social. El impulso normativo se plantea cuando un aspecto concreto de la convivencia es susceptible de lesionar o poner en peligro los derechos y libertades de los ciudadanos. Es entonces cuando el legislador debe actuar para preservar esos bienes empleando los medios previstos en el ordenamiento jurídico.

En concreto, en los últimos años estamos experimentando una revolución tecnológica acelerada, especialmente en el ámbito de las comunicaciones, donde el correo ordinario ha ido dando paso al correo electrónico como medio de comunicación predominante, ha sido posible sustituir las conversaciones presenciales por las telefónicas entre personas ubicadas en distintos lugares, e incluso se ha logrado establecer comunicaciones instantáneas escritas o virtualmente presenciales a través de videoconferencia. Estos ejemplos no parecen sino el principio de una gran transformación en los próximos años. De igual forma, en el ámbito de la información encontramos manifestaciones de la nueva dimensión digital con la

aparición de instrumentos como los *e-readers*[1], las *phablets*[2] o los *smartwatches*,[3] que permiten la lectura de datos en instrumentos de poco peso, sin necesidad de imprimirlos en un recurso natural limitado como el papel; o con la generalización del uso de Internet, que se ha convertido en la fuente más importante de información del mundo y en un medio accesible para cualquier persona. Dicho de otro modo, la información es susceptible de llegar a cualquier lugar y ya no sólo a

---

[1] Se entiende por *e-reader* el anglicismo de lector de libros electrónicos, que son conocidos como los *e-book* o *ebook* y son versiones electrónicas o digitales de un libro. Definición disponible en https://es.wikipedia.org/wiki/Libro_electrónico, consultado el 11 de septiembre de 2016.

[2] Es comúnmente aceptado el término *phablet* recogido en la *Wikipedia*, como contracción inglesa entre *phone* y *e*, también conocido en español como tabléfono o tabletófono, "*denominaciones informales utilizadas para designar dispositivos electrónicos móviles o portátiles, con pantallas táctiles entre 5,3 y 7 pulgadas aproximadamente y con múltiples prestaciones de hardware y software*", combinando "*las funcionalidades y capacidades de un teléfono inteligente con una tableta, y puede incorporar un estilete digital*". Definición disponible en https://es.wikipedia.org/wiki/Tabléfono consultado el 11 de septiembre de 2016.

[3] Los *smartwatches* (del inglés, reloj inteligente) son relojes de pulsera dotados "*con funcionalidades que van más allá de las de uno convencional*", que "*incorpora un conjunto de componentes electrónicos junto con un microprocesador capaz de ejecutar aplicaciones informáticas gracias a las cuales el propietario puede acceder a internet, consultar su correo electrónico, realizar y recibir llamadas, monitorizar y cuantificar su actividad diaria, ejecutar determinadas apps"*, entre otras funciones. En este sentido se define en https://es.wikipedia.org/wiki/Reloj_inteligente y http://www.quees.info/que-es-un-smartwatch.html, consultado el 4 de enero de 2017.

través de un ordenador, sino con cualquier herramienta con conexión a Internet.

El progreso tecnológico y la digitalización de la información han influido en tantos ámbitos que incluso se ha defendido la existencia de un nuevo mundo digital, una nueva sociedad o una cibersociedad[4], que algunos autores consideran distinta al mundo analógico tradicional[5].

Sin embargo, la universalidad y transnacionalidad de estos nuevos medios de comunicación e información, con todas sus bondades, no deja de ir acompañada de importantes riesgos para las libertades de las personas, incluso para el Estado de Derecho, que tiene como una de sus funciones esenciales la de garantizar la eficacia y protección de esas libertades, las cuales ahora pueden verse lesionadas por nuevos medios carentes todavía de una normativa suficientemente eficaz. Esos riesgos tienen la nota común de que su procedencia radica en bancos de datos estructurados y combinados con los sistemas de comunicación[6], tal y como veremos en el presente trabajo.

---

[4] LÓPEZ ZAMORA, P., *El Ciberespacio y su Ordenación*, ed. Difusión Jurídica y Temas de Actualidad, Madrid, 2006, p. 95.

[5] MORÓN LERMA, E., *Internet y Derecho Penal: <<Hacking>> y otras conductas ilícitas en la red,* ed. Aranzadi, segunda edición, Navarra, 2002, p. 21.

[6] CASTILLO JIMENEZ, C., *Protección del Derecho a la Intimidad y Uso de las Nuevas Tecnologías de la Información,* Universidad de Huelva, Huelva, 2001, p. 36.

Frente a los peligros que entraña el uso de las nuevas tecnologías, no parece legítima la imposición de restricciones que vayan más allá de las existentes en el mundo físico o real, lo cual no excluye que, como señala ROMEO CASABONA[7], cuando se impongan limitaciones, se tenga siempre presente la potencialidad lesiva de las TIC[8], o ICT[9] en el mundo anglosajón, por la fácil y rápida expansión de contenidos ilícitos a través de ellas.

El desarrollo de estas tecnologías ha traído ataques contra los terminales y sistemas de comunicación, pero las propias TIC también se han empleado como instrumento para delinquir y atentar sobre los bienes jurídicos que ya eran objeto de tutela en nuestro ordenamiento. Dicho en otras palabras, las posibilidades que ofrecen las TIC constituyen un nuevo bien susceptible de protección, pero también se han erigido como un nuevo medio para delinquir contra los bienes

---

[7] ROMEO CASABONA, C. M., "Derecho Penal y libertades de expresión y comunicación en Internet", en ARMAZA ARMAZA, Emilio José (Coord.) y VVAA, *La Adaptación del Derecho Penal al Desarrollo Social y Tecnológico*, ed. Comares, Granada, 2010, p. 321.

[8] MIRÓ LLINARES, F., *El Cibercrimen,* ed. Marcial Pons, Madrid, 2012, p. 25: "*se viene admitiendo que se incluyen dentro de las TIC, tanto las redes (entre las cuales destaca Internet pero también se incluyen las de telefonía móvil y otras redes telemáticas), como las terminales (entre las que destacan los sistemas informáticos consistentes en ordenadores personales, pero también comienzan a ser gran vehículo de comunicación las consolas) y los servicios, entre los que destacan todavía la descarga de archivos en sitios de intercambio gratuito y en webs de pago, pero también el comercio electrónico, la banca electrónica, la realización electrónica de actividades relacionadas con la Administración Pública y, cada vez más, las redes sociales*".

[9] Siglas correspondientes a "*Information and communications technology*".

jurídicos tradicionales.

Por ello, en el ámbito penal, la evolución de la política criminal en los últimos años plantea la necesaria renovación legislativa, pues los mecanismos de tutela existentes no resultan plenamente satisfactorios para dar respuesta a los problemas derivados de estas nuevas tecnologías. Tal y como indica BORJA JIMÉNEZ[10], surgen nuevas cuestiones político-criminales que no pueden ser resueltas con los mecanismos del Derecho Penal clásico. Así, el sistema de comunicaciones ha avanzado hasta el punto de afectar a cada ciudadano y a las instituciones, modificando la estructura de los Estados, y se han multiplicado las transacciones económicas. También se ha producido una globalización económica y cultural. Por tanto, el nuevo tipo de sociedad contiene el progreso continuo del conocimiento, donde las formas de vida son cada vez más complejas bajo el dominio de la informática. En resumen, los medios tradicionales son insuficientes para la protección de los equipos y sistemas informáticos por una parte y, por otra, para la salvaguarda de los bienes jurídicos que se puedan ver afectados por el uso indebido de la tecnología. Como señala QUERALT JIMÉNEZ[11], la informática opera siguiendo factores lógicos y no físicos, razón por la cual las ideas jurídicas conocidas hasta ahora no son adecuadas para repeler los ataques a los bienes jurídicos tradicionales como pueda ser la

[10] BORJA JIMÉNEZ, E., *Curso de política criminal*, ed. Tirant lo Blanch, segunda edición, Valencia, 2011, p. 273-276.

[11] QUERALT JIMÉNEZ, J. J., *Derecho penal español. Parte especial*, ed. Tirant lo Blanch, primera edición, Valencia, 2015, p. 338.

intimidad.

Ahora bien, el hecho de que nos encontremos ante un campo nuevo para el Derecho penal no implica que, existiendo una conducta de riesgo sobre las nuevas tecnologías, necesariamente deba emplearse el instrumento punitivo. En este punto debe tenerse presente el principio de intervención mínima[12], principio informador del Derecho penal que, por ser uno de los fundamentales de esta disciplina, también tiene que ser respetado a la hora de tipificar estas conductas relativas a las nuevas tecnologías.

Precisamente este principio ha sido considerado tanto expresa como tácitamente por el legislador en las continuas reformas del Código Penal. Así, en cuanto a las modificaciones que han afectado a los delitos tecnológicos, consta en la Exposición de Motivos del Código Penal de 1995, aprobado por la Ley Orgánica 10/1995, de 23 de noviembre: "*se ha afrontado la antinomia existente entre el*

[12] Tal y como sabemos, este principio significa, según recuerda QUINTERO OLIVARES, que "*el Derecho penal debe actuar lo menos posible y sólo para el control de las conductas que de otro modo se harían insoportables para la convivencia*" (QUINTERO OLIVARES, G., "La autotutela, los límites al poder sancionador de la Administración Pública y los principios inspiradores del Derecho Penal", en *RAP*, nº 126, 1991,p. 274, disponible en https://dialnet.unirioja.es/descarga/articulo/17106.pdf, consultado el 4 de enero de 2017). Así, conforme resume LUZÓN CUESTA, se atribuye al Derecho penal un carácter subsidiario, entendiendo que es la *última ratio*, debiendo intervenir cuando se revelen como ineficaces los demás medios de tutela y sanción con los que cuente el Estado de Derecho para proteger los bienes jurídicos, y se le asigna un carácter fragmentario, según el cual sólo debe amparar los más fundamentales y frente a los ataques más intolerables (LUZÓN CUESTA, J. M., *Compendio de Derecho Penal. Parte General*, ed. Dykinson, Madrid, 2016, p. 26).

*principio de intervención mínima y las crecientes necesidades de tutela en una sociedad cada vez más compleja, dando prudente acogida a nuevas formas de delincuencia, pero eliminando, a la vez, figuras delictivas que han perdido su razón de ser*", y se ha argumentado implícitamente sobre la *ultima ratio* en la Exposición de Motivos del Proyecto de la Ley Orgánica 5/2010 al mencionar que "*El objetivo del legislador ha sido siempre avanzar en el tratamiento de aquellas materias que han ido conformándose como objeto de especial preocupación social tras la promulgación del Código vigente*"[13] y en el Preámbulo de la Ley Orgánica 1/2015 donde se expone que "*el transcurso del tiempo y las nuevas demandas sociales evidencian la necesidad de llevar a cabo determinadas modificaciones de nuestra norma penal*" y "*se suprimen aquellas otras infracciones que, por su escasa gravedad, no merecen reproche penal*"[14].

Todo ello implica que sólo cuando las conductas o ataques relacionados con las nuevas tecnologías vulneren realmente los intereses que protege el Derecho penal y, además, atenten de la manera más grave contra esos intereses, esas acciones en sentido amplio pueden competer a esta disciplina, no procediendo su aplicación frente a cualquier conducta de riesgo relacionada con los

[13] Texto del Proyecto de Ley Orgánica por la que se modifica la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal, publicado en el *BOCG*, Congreso de los Diputados, el 27 de noviembre de 2009. Núm. 52-1. La citada previsión no fue mantenida en el texto definitivo de la LO 5/2010.

[14] Texto de la Ley Orgánica 1/2015 por la que se modifica la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal, publicado en el *BOE* el 31 de marzo de 2015. Núm. 77.

mencionados sistemas o tecnologías. De esta forma, con anterioridad a la regulación del *hacking* en el Código Penal español, la Sentencia del Juzgado de lo Penal 2 de Barcelona, de 28 de mayo de 1999, exponía que las conductas de acceso no autorizado a un sistema informático ajeno, "*en cuanto suponen de agresión contra el interés del titular de un determinado sistema de que la información que en él se contiene no sea interceptada, resultan tanto más reprobables, y aún merecedoras de sanción penal si -como suele ser lo habitual- atentan contra sistemas o equipos informáticos particularmente relevantes que, por razón del contenido de la información que procesan o almacenan y por las funciones que tienen asignadas en el seno de las relaciones jurídicas, económicas y sociales, afectan gravemente a un interés supraindividual o colectivo, de manera que plantear en esta sede una adecuada tutela penal autónoma frente al intrusismo informático no puede en modo alguno considerarse un exceso de reacción penal*"[15].

No obstante, tal y como indica DE URBANO CASTRILLO, en los últimos años el legislador viene mostrando una clara voluntad de huida hacia el Derecho penal, especialmente en los fenómenos delictivos o sociales de trascendencia mediática, abandonando la idea

[15] Sentencia del Juzgado de lo Penal 2 de Barcelona, de 28 de mayo de 1999, Procedimiento Abreviado 130/99-E, Pte. Ilmo. Sr. D. Juan Carlos Llavona Calderón, disponible en http://www.bufetalmeida.com/58/caso-hispahack-1-absolucion-de-presuntos-hackers-la-sentencia.html, consultado el 23 de febrero de 2012, FD 1º.

del Derecho penal como *ultima ratio*[16] para convertirlo en el instrumento de respuesta en los casos de alarma social. A pesar de esta instrumentalización, el carácter global y supranacional de las TIC pone en entredicho que el sistema penal tenga capacidad suficiente para una eficaz regulación[17] de estas nuevas relaciones sociales.

En cualquier caso, el esfuerzo interpretativo que estaban asumiendo los órganos jurisdiccionales para evitar la impunidad de estas nuevas acciones, con la consecuente puesta en peligro de la seguridad jurídica y por lo tanto del principio de legalidad, exigía una revisión legislativa, no sólo en el ámbito nacional, sino fundamentalmente en el internacional, atendido el potencial alcance transfronterizo de estas conductas.

Con este punto de partida, el presente trabajo constituye un análisis de la necesaria reforma operada por la LO 5/2010 en el artículo 197 del Código Penal, en concreto en su apartado 3, donde se han introducido las conductas de acceso ilícito a sistemas informáticos o *hacking*, al que se dedican las siguientes páginas y que tras la entrada en vigor de la Ley Orgánica 1/2015 se han ubicado en su artículo 197 *bis* 1. Por tanto, por su ubicación y con los matices que expondremos, guarda relación con los comportamientos penalmente

---

[16] DE URBANO CASTRILLO, E., "Los delitos informáticos tras la reforma del CP de 2010", en VVAA, *Delincuencia informática. Tiempos de cautela y amparo*, ed. Aranzadi, primera edición, Navarra, 2012, p. 21.

[17] SÁNCHEZ MAGRO, A., "El ciberdelito y sus implicaciones procesales", en GARCÍA MEXÍA, P. (Dir.), y VVAA. *Principios de Derecho de Internet*, ed. Tirant Lo Blanch, Valencia, 2005, epígrafe 6.

relevantes susceptibles de vulnerar el derecho a la intimidad o la propia imagen a través de las nuevas tecnologías.

Para llevar a cabo el análisis, el trabajo se ha dividido en un primer capítulo dedicado a los antecedentes y evolución del *hacking*, lo que nos sirve para determinar la importancia del tema, para a continuación hacer una breve referencia al Derecho comparado europeo con el objetivo de contrastar la normativa española y las legislaciones que regulan la materia con mayor o menor sistematización. El bien jurídico protegido en este delito es el siguiente punto, contrastando la intimidad y sus críticas con la seguridad de los sistemas informáticos, siguiendo con los elementos que lo integran, las formas de aparición, sus relaciones concursales, los tipos agravados y la responsabilidad de las personas jurídicas, finalizando con las conclusiones.

# CAPÍTULO I.

# ANTECEDENTES Y EVOLUCIÓN DEL *HACKING.*

## *1. INTRODUCCIÓN.*

En el presente capítulo se exponen unos conceptos previos al estudio del delito de *hacking*, comenzando por un acercamiento a los primeros pasos de Internet y su vinculación progresiva al bien jurídico intimidad. También se van a mostrar algunos de los conceptos relativos a la categoría donde se considera que tienen cabida estas conductas dentro de nuestro ordenamiento jurídico y las características de la delincuencia informática.

Una vez fijado este punto de partida, se relatan las distintas manifestaciones iniciales del acceso ilícito a sistemas informáticos ajenos y la respuesta en el ámbito normativo internacional.

Por último, se concluye el presente apartado con el análisis conceptual del *hacking* propiamente dicho y su consideración en el ordenamiento jurídico español.

### *1.1 El nacimiento de la red y su vinculación con la intimidad.*

Históricamente nos encontramos en un momento de cambio que hace que las tradicionales comunicaciones presenciales sean sustituidas por comunicaciones virtuales en cualquier parte del mundo, que el intercambio de información sea instantáneo o que cualquier persona pueda acceder a la fuente más importante de información jamás conocida: Internet, que se ha definido de forma

generalmente aceptada como un "*sistema de información global que: (i) Está conectado lógicamente por direcciones únicas, basadas en el Internet Protocol (IP) y sus extensiones o añadidos consecutivos. (ii) Puede soportar comunicaciones usando el conjunto de protocolos TCP/IP o sus extensiones o añadidos consecutivos, así como otros Protocolos IP compatibles. (iii) Provee, usa o hace accesible, cualquiera de los niveles de capa superior públicos o privados de las comunicaciones y relacionados con la infraestructura descrita aquí*"[18]; o también como "*una red internacional de computadoras interconectadas que permite a millones de personas se comuniquen entre sí en el <<ciberespacio>> y acceder a grandes cantidades de información de todo el mundo*"[19].

Es por ello que podemos referirnos a nuestra sociedad actual como una sociedad de información, a la que se ha referido CASTELLS como un "*nuevo sistema tecnológico, económico y social. Una economía en la que el incremento de productividad no depende del incremento cuantitativo de los factores de producción (capital, trabajo, recursos naturales), sino de la aplicación de conocimientos e información a la gestión, producción y distribución, tanto en los*

[18] Definición ofrecida por el *Federal Networking Council* de Estados Unidos en su Resolución de 24 de octubre de 1995, disponible en https://www.nitrd.gov/fnc/Internet_res.aspx, consultado el 13 de septiembre de 2016.

[19] Sentencia del Tribunal Supremo de Estados Unidos Reno vs. American Civil Liberties Union, de 26 de junio de 1997, disponible en http://caselaw.lp.findlaw.com/cgi-bin/getcase.pl?court=us&navby=case&vol=521&invol=844, consultado en 13 de septiembre de 2016.

*procesos como en los productos*"[20].

Por tanto, actualmente estamos experimentando una nueva revolución, la tecnológica, que obedece a la microelectrónica, informática, telecomunicaciones o la ingeniería genética, entre otros factores y, dentro de toda esta transformación el epicentro lo marca Internet. Empleando los términos del Informe Bargemann, emitido en el seno de la UE en 1994, estamos ante "*una nueva revolución industrial tan importante y de tanto alcance como sus predecesoras. Se trata de una revolución basada en la información, por sí misma la expresión del conocimiento humano*"[21]. El poder ya no reside en la fuerza física, sino que, como señala GONZÁLEZ NAVAJAS, en las sociedades informatizadas el poder recae en el uso de las informaciones, que permiten influir y controlar las conductas individuales sin necesidad de medios coactivos[22].

---

[20] CASTELLS, M., *La era de la información*. *Economía, sociedad y cultura. Volumen II: El poder de la identidad,* Alianza Editorial, Madrid, 1998, p. 45.

[21] El denominado Informe Bangemann (Bangemann Report), encargado por el Consejo Europeo y emitido el 26 de mayo de 1994, establece en su primer capítulo ("*The information society - new ways of living and working together*"): "*Throughout the world, information and communications technologies are generating a new industrial revolution already as significant and far-reaching as those of the past. It is a revolution based on information, itself the expression of human knowledge*". Consultado el 4 de enero de 2016 en http://ec.europa.eu/archives/ISPO/infosoc/backg/bangeman.html.

[22] GÓMEZ NAVAJAS, J., *La protección de datos personales. Un análisis desde la perspectiva del Derecho Penal*. Editorial Aranzadi, Navarra, 2005, p. 36.

En este marco social, tecnológico y revolucionario, existen múltiples factores que han favorecido la rápida expansión de las conductas que se sirven de las nuevas tecnologías para producir resultados dañosos. Como señala BARRIO ANDRÉS, cada día surgen nuevos fallos en los sistemas informáticos y su protección requiere numerosos y costosos medios, por lo que cualquier usuario de Internet se convierte en víctima potencial de estos ilícitos. Además, estos comportamientos muchas veces no se descubren o se descubren tarde o por azar, produciéndose una "macro-victimización"[23]. Por ello, no debe decaer la tutela penal de los bienes jurídicos frente a las graves intromisiones por el hecho de que los medios de ataque estén en continua renovación[24].

Por estos motivos, para lograr una política criminal eficaz será preciso concretar cuáles son las cuestiones que se suscitan en torno a la facilidad de comisión, la dificultad de su persecución, el anonimato de Internet, la obtención de rápidos beneficios, o la transnacionalidad, que no son sino algunos de los obstáculos para la persecución que se unen a otros como el interés en no dar publicidad a estos ataques, tanto desde el sector empresarial privado, en muchos casos para conservar la confianza de los clientes, como desde el sector público,

---

[23] BARRIO ANDRÉS, M., "El régimen jurídico de los delitos cometidos en Internet en el derecho español tras la reforma penal de 2010", en en VVAA, *Delincuencia informática. Tiempos de cautela y amparo*, ed. Aranzadi, primera edición, Navarra, 2012, p. 35.

[24] En este sentido, ANARTE BORRALLO, E. y DOVAL PAIS, A., "Límites de la ley penal a propósito del nuevo delito de intrusión informática", en *RGDP*, noviembre 2012, nº 18, p. 3.

fundamentalmente por motivos de seguridad.

Con carácter previo a referirnos al concepto de Derecho penal informático, conviene tener presente la revolución tecnológica que comienza con los orígenes de Internet en 1958, momento en el que el Departamento de Defensa de Estados Unidos creó la Agencia de Proyectos de Información Avanzada para superar tecnológicamente a la antigua Unión Soviética, que ya había lanzado el Sputnik en 1957. Esta Agencia pretendía captar recursos del mundo universitario para su aplicación al ámbito militar. En este ámbito universitario, en 1962 Paul Barán explicaba las redes de conmutación de paquetes en su libro *Las Redes de Comunicación Distribuidas*, idea que se materializaría en ARPANET, como primer programa de conmutación de paquetes en 1969, que se hizo público en 1972, momento en el que también se introdujo su primera aplicación en él: el correo electrónico. ARPANET tuvo su evolución natural hacia la conexión con otros ordenadores, apareciendo la red de redes: Internet. Así, en 1973 los informáticos Kahn y Cerf de la Universidad de Stanford, crearon los protocolos de comunicación comunes, y en 1983 nace Internet tal y como es conocido actualmente, cuando el Departamento de Defensa de los Estados Unidos utiliza el protocolo TCP/IP (*Transmission Control Protocol/Internet Protocol*) en su red ARPANET. La red se expandió a medida que se incorporaron nuevos nodos y se fue reconfigurando, siendo hito fundamental la aportación de Tim Bernes Lee en 1992 creando la *World Wide Web* con tres nuevos instrumentos: el HTML (*Hypertext Markup Language*), HTP

(*Hypertext Transfer Protocol*) y el programa cliente *Web Browser*. Tras esta evolución, se nos presenta Internet como una integración descentralizada[25], la máxima síntesis de la colaboración entre los medios de comunicación modernos y la tecnología informática[26].

De esta forma, refiriéndonos al ámbito jurídico, señala ANARTE BORRALLO cómo en un principo las preocupaciones se centraban en los riesgos que el uso de los sistemas informáticos suponían para la intimidad[27]. La tutela de la *privacy* aparece en los años sesenta, como consecuencia del archivo gubernamental de los datos personales de los ciudadanos y su ingente acumulación, lo que trajo la preocupación sobre el uso que se podía hacer de esos datos. Surge así el concepto del derecho a la *privacy*, que supera el tradicional derecho a la intimidad para referirse a la acumulación de datos y al uso que se puede hacer de ellos, materia que en un primer momento será tratada en el ámbito civil y administrativo y, poco a poco, se ampliará para comprender el ámbito penal.

En la década de los setenta, comienza la extensión del uso de ordenadores en el ámbito empresarial y, con ella, la delincuencia económica relacionada con ellos. En este período estas formas de

---

[25] LÓPEZ ZAMORA, P., *El ciberespacio ...*, *cit*., nota 4, p. 43.

[26] MENÉNDEZ MATO, J. C. y GAYO SANTA CECILIA, M. E., *Derecho e informática: ética y legislación*, ed. Bosch Editor, Barcelona, 2014, p. 26.

[27] ANARTE BORRALLO, E., "Incidencia de las nuevas tecnologías en el sistema penal", en *Derecho y conocimiento: anuario jurídico sobre la sociedad de la información y del conocimiento*, nº 1, ed. Facultad de Derecho de la Universidad de Huelva, Huelva, 2001, p. 194.

delincuencia económica son las que predominan a través de la informática e integran lo que se puede identificar como delito informático en un primer momento.

En los años posteriores el uso de los ordenadores se globaliza y no se reduce al ámbito empresarial. Así, en los años ochenta, con el uso extendido de los ordenadores personales, aparecerá la piratería del *software* y, con ella, las infracciones contra la propiedad intelectual, que se incrementan especialmente en los años noventa, cuando abarcará también música o películas. De esta forma, la aparición de Internet y su expansión también supone una nueva herramienta de difusión de contenidos ilícitos como la pornografía infantil o la apología del racismo o la xenofobia, o incluso actuaciones contra la seguridad del Estado a través del terrorismo cibernético.

Por ultimo, en el uso de las nuevas tecnologías actualmente concurren una serie de factores, como es (i) un precipitado acceso a ellas, lo que facilita la causación de daños imprudentes en sistemas informáticos, la obstaculización en su normal funcionamiento o incluso el acceso ilícito a ellos; (ii) una reducción o incluso supresión de privacidad motivada por la acumulación de datos personales en los distintos sistemas, públicos y privados; y (iii) las deficiencias en los propios equipos y redes informáticas que facilitan la vulneración de su privacidad, de los derechos salvaguardados a través de ellos o el adecuado desarrollo de su entorno. De esta forma, tal y como señala DE LA MATA BARRANCO, resultan ser numerosos los potenciales ataques a través de la informática, especialmente tras la expansión y

uso generalizado de Internet, quedando pocos espacios de la vida que no se vean influidos por procesos de tratamientos de datos, que facilitan también la comisión de delitos tradicionales. Así, en el ejemplo citado por este autor, del que accede a un sistema informático de un hospital para alterar la distribución de medicamentos, podría llegar a apreciarse una tentativa de asesinato[28], ejemplo que podría trasladarse a cualquier otro sistema público o privado y relacionarse con cualquier otro bien jurídico protegido.

Por ello, podemos concluir que hoy en día prácticamente cualquier delito es susceptible de cometerse o verse favorecido a través de estas nuevas herramientas de la información y la comunicación.

### *1.2 El concepto de Derecho penal informático.*

Con el fin de dar cobertura al campo relativo a las nuevas tecnologías, en un intento por unificar los criterios de estudio se hace preciso delimitar diferentes conceptos y el ámbito de la materia que nos ocupa.

En el seno de la UE[29], la ciberdelincuencia se ha definido

---

[28] DE LA MATA BARRANCO, N. J., "Los delitos vinculados a las tecnologías de la información y comunicación en el Código Penal: panorámica general", en *Cuadernos penales José María Lidón*, *nº 4. Delito e informática: algunos aspectos*, Universidad de Deusto, Bilbao, 2007, p. 42.

[29] Concepto recogido en la "*Comunicación de la Comisión al*

como "*actividades delictivas realizadas con la ayuda de redes de comunicaciones y sistemas de información electrónicos o contra tales redes y sistemas*", desglosándola en tres tipos de conductas: (i) las "*formas tradicionales de actividades delictivas, pero utilizando internet para cometer delitos (como el fraude o la falsificación)*"; (ii) "*la publicación de contenidos ilegales, como material que incite al terrorismo, la violencia, el racismo o la xenofobia o al abuso sexual a menores*"; y (iii) los "*delitos específicos de las redes electrónicas, que incluyen nuevos delitos, a menudo de amplia variedad y a gran escala, desconocidos antes de internet. En estos casos, los delincuentes atacan sistemas de información, en ocasiones amenazando infraestructuras informáticas críticas de un Estado, por lo que la amenaza se dirige también a sus ciudadanos*".

Por tanto, aunque como indica ANARTE BORRALLO en el estudio de la cibercriminalidad no existe un único concepto ni figura delictiva empleándose en cada esfera con diversos sentidos[30], tal y como se ha expuesto, cobra especial relevancia la distinción entre delitos cometidos a través de la informática y los delitos en los que la informática es en sí misma el objeto del delito. La criminalidad informática comprende las conductas tipificadas en el Código Penal

---

*Parlamento Europeo, al Consejo y al Comité de las Regiones: Hacia una política general de lucha contra la ciberdelincuencia*" (COM (2007) 267 final de 22 de mayo de 2007), disponible en http://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=URISERV:l14560&from=ES, consultado el 10 de enero de 2017.

[30] ANARTE BORRALLO, E., "Incidencia de las nuevas tecnologías ...", *cit*., nota 27, p. 199.

vinculadas con la informática, ora siendo su objeto la informática, ora siendo la informática el medio de comisión, por lo que la doctrina viene defendiendo, cada vez más, la definición en la legislación penal del nuevo bien jurídico vinculado a la informática. Además, estos cibercrímenes tienen cuatro rasgos característicos: fácil comisión; escasos recursos requeridos en relación con el perjuicio que se causa; se pueden cometer en distinta jurisdicción sin encontrarse físicamente en ella; y, por último, se benefician de las lagunas normativas en determinados Estados, que han sido denominados por ello paraísos cibernéticos[31], entre los que generalmente se ubica a Irán, Filipinas o Tailandia[32].

Si bien el Derecho penal tradicional ha logrado superar fronteras para poder perseguir los delitos con elementos de extranjería (por ejemplo, tráfico de drogas o de personas), la cibercriminalidad supone un nuevo reto de difícil solución, que se ve incrementado con nuevos elementos, no sólo por los continuos cambios en las nuevas tecnologías, sino también en el perfil del delincuente, que pasa de ser joven de clase media obsesionado por controlar los medios, o empleados con ánimo de venganza y sin ánimo de lucro, hacia un

---

[31] DE LA CUESTA ARZAMENDI, J. L., PÉREZ MACHÍO, A. I. y SAN JUAN GUILLÉN, C., "*Aproximaciones Criminológicas a la Realidad de los Ciberdelitos*", en DE LA CUESTA ARZAMENDI, J. L. (Dir.), y VVAA, *Derecho Penal Informático*, ed. Civitas, Pamplona, 2010, p. 80.

[32] RIQUERT, M. A., "Protección contra la delincuencia informática en el MERCOSUR", en http://riquertdelincuenciainformatica.blogspot.com/2007/11/proteccin-contra-la-delincuencia.html, Universidad Nacional de Mar del Plata, 11 de noviembre de 2007, consultado el 4 de abril de 2017.

perfil de persona con conocimientos informáticos[33].

Por ello, la heterogeneidad de estas conductas, su especial naturaleza y las dificultades de persecución han exigido la armonización del Derecho penal material entre los distintos Estados y las consiguientes reformas legislativas, justificando la modificación normativa tal y como se expondrá en los siguientes epígrafes.

En líneas generales, como indican ANARTE BORRALLO y DOVAL PAIS, las iniciativas legislativas se han llevado a cabo desde el punto de vista del "*Derecho penal de la seguridad*", dirigido a luchar contra las perturbaciones sistemáticas, es decir, "*ataques a gran escala, en la jerga comunitaria- derivadas de nuevos avances tecnológicos que, en este caso, afectan a aspectos claves de la sociedad de la información y del conocimiento –como la integridad de la información contenida en sistemas informáticos aislados o conectados o de los propios sistemas- y, dada su imbricación en la vida diaria, la confianza de la colectividad en el vigente sistema social"*[34].

Así pues, en una primera aproximación la doctrina se ha referido al Derecho informático como "*conjunto de normas jurídicas que regulan la utilización de los bienes y servicios informáticos en la*

---

[33] DE LA CUESTA ARZAMENDI, J. L. y PÉREZ MACHÍO, A. I. y SAN JUAN GUILLÉN, C., "*Ciberdelincuentes y Cibervíctimas*", en DE LA CUESTA ARZAMENDI, J. L. (Dir.), y VVAA, *Derecho Penal Informático*, ed. Civitas, Pamplona, 2010, p. 101.

[34] ANARTE BORRALLO, E. y DOVAL PAIS, A., "Límites de la ley penal ...", *cit*., nota 24, p. 3.

*sociedad*"[35]. Esta descripción genérica parece acertada como premisa, por cuanto se presenta como suficientemente amplia para dar cabida a cualquier rama del Derecho que se ocupe de esta materia, siendo el problema doctrinal la definición del Derecho penal informático, especialmente por el continuo cambio de las nuevas tecnologías y sus afecciones a distintos bienes jurídicos protegidos. Por ello, tal y como indica DE LA MATA BARRANCO, no resulta muy acertado partir de un concepto propio a modo de rama dentro del Derecho penal como en otros casos relativos al patrimonial, sexual o a la Administración de justicia, de tal manera que pudiera hablarse también de un delito contra la informática. Más bien parece correcto pensar con este autor que un concepto ajustado a nuestro ordenamiento jurídico haría referencia a "*conductas típicas vinculadas, por el medio comisivo, el objeto del ataque, etc., al ámbito de la informática o de la cibernética, al ámbito del mundo digital*", es decir, serían conductas típicas, "*al margen de consideraciones político-criminales sobre posibles lagunas de penalidad que sea necesario cubrir*"[36].

Es concretamente la evolución de las nuevas tecnologías citada en el punto anterior y las conductas delictivas relacionadas con ellas lo

---

[35] HERNÁNDEZ DÍAZ, L., "Aproximación a un Concepto de Derecho Penal Informático", citando a ZICCARDI, nota 2, en DE LA CUESTA ARZAMENDI, J. L. (Dir.) y VVAA, *Derecho Penal Informático*, ed. Civitas, Pamplona, 2010, p. 31, citando a ZICCARDI, G., "Il diritto dell'informatica", en PATTARO, E. (Dir.), *Manuale di diritto dell'informatica e delle nuove tecnologie*, ed. Clueb, Bolonia, 2000, p. XIII.

[36] DE LA MATA BARRANCO, N. J., "Los delitos vinculados a las tecnologías ...", *cit*., nota 28, p. 44.

que ha motivado que parte de la doctrina prefiera negar el concepto de delito informático y se haya referido a delincuencia informática, criminalidad informática o delitos informáticos en general.

De esta forma se elude el problema de que, como indica HERNÁNDEZ DÍAZ, con la utilización del término delito informático se identifique con su realidad positiva, por cuanto la referencia es inexistente en la ley penal[37], mismo problema que surgiría con el empleo de la categoría Derecho penal informático. Así, para algunos autores como MENÉNDEZ MATO y GAYO SANTA CECILIA, se puede entender como delitos informáticos en general "*aquellas conductas que a través de medios tecnológicos o informáticos conculcan lo establecido en el ordenamiento jurídico*"[38]. Sin embargo, con su referencia a los medios, no incluyen en su definición los supuestos en los que el sistema informático es el objeto de ataque, tal y como sucedería en el caso del *hacking*. Por ello parece más acertada la referencia a delincuencia informática o criminalidad informática como los "*comportamientos en los que un sistema informático sea el medio para lesionar un bien jurídico, cualquiera, y todos aquéllos en que dicho sistema sea él mismo el propio objeto sobre el que recae la acción delictiva*", siguiendo así el concepto mayoritario que resume HERNÁNDEZ DÍAZ[39], definición que

---

[37] En este sentido, HERNÁNDEZ DÍAZ, L., "Aproximación a un Concepto ...", *cit*., nota 35, p. 42.

[38] MENÉNDEZ MATO, J. C. y GAYO SANTA CECILIA, M. A., *Derecho e informática ...*, *cit*., nota 26, p. 319.

[39] HERNÁNDEZ DÍAZ, L., "Aproximación a un Concepto ...", *cit*., nota

también parece aplicable al de delitos informáticos en general, dando así cabida dentro de la categoría también a los equipos, redes o sistemas informáticos como objeto del ataque.

En consecuencia, la citada terminología evita la mención al delito informático en un sentido estricto, que plantea el problema de que sólo serían "*aquellas conductas ilícitas tipificadas como tales en las correspondientes leyes penales*"[40]. De tal manera que no podemos localizar un grupo específico de delitos informáticos en la legislación española, cuya creación sería, por tanto, ficticia y constituiría como señala BARRIO ANDRÉS, una nueva clase de ilícitos no autorizada por el legislador ni exigida por la naturaleza de las cosas[41].

Por tanto, en nuestro sistema jurídico nos encontramos con el hecho de que no existe una ley como la chipriota, portuguesa o inglesa, o un título específico en el Código Penal para los delitos informáticos como en el caso de Bulgaria o Croacia. Como señala SÁNCHEZ DOMINGO, las razones las encontramos en que el legislador ha optado por agrupar las conductas atendiendo al bien jurídico protegido y los ilícitos penales cometidos a través de las nuevas tecnologías son tan variados y pueden afectar a tantos bienes

---

35, p. 43, citando a ÁLVAREZ VIZCAYA, M., "Consideraciones político criminales sobre la delincuencia informática: el papel del Derecho penal en la red", en *Internet y Derecho penal. Cuadernos de Derecho Judicial*, Madrid, 2001, p. 257.

40 MENÉNDEZ MATO, J. C. y GAYO SANTA CECILIA, M. A., *Derecho e informática ...*, *cit*., nota 26, p. 319.

41 BARRIO ANDRÉS, M., "El régimen jurídico de los delitos ...", *cit*., nota 23, p. 34.

jurídicos que no ha sido posible encuadrarlos en una única categoría[42].

No obstante, algunos autores como ROMEO CASABONA han ofrecido una definición de cibercrimen como "*el conjunto de conductas relativas al acceso, apropiación, intercambio y puesta a disposición de información en redes telemáticas, de las cuales constituyen su entorno comisivo, perpetradas sin el consentimiento o autorización exigibles o utilizando información de contenido ilícito, pudiendo afectar a bienes jurídicos diversos de naturaleza individual o supraindividual*", de esta forma el concepto abarca una nueva generación de delitos vinculada a los sistemas informáticos[43].

De un modo más simplificado SIEBER se refiere a la delincuencia informática como "*cualquier comportamiento ilegal, al margen de la ética o realizado sin autorización en el marco del proceso o transmisión de datos*"[44], o COLÁS TURÉGANO[45] a los

---

[42] SÁNCHEZ DOMINGO, M. B., "Delincuencia Informática y el delito de intrusismo informático: aspectos de su regulación en instrumentos normativos europeos y su transposición al Código Penal español acorde a la LO 5/2010 de reforma de Código Penal español", en *RGDP de Iustel*, nº 18, 2012, texto íntegro del artículo disponible en http://www.iustel.com/v2/revistas/detalle_revista.asp?id_noticia=412629, consultado el 6 de enero de 2017. *Vid*., Capítulo II, epígrafe 3.

[43] ROMEO CASABONA, C. M. (Dir.) y VVAA, *El cibercrimen nuevos retos jurídico-penales, nuevas respuestas político-criminales*, ed. Comares, Granada, 2006, p. 11.

[44] SIEBER, U., "Documentación para una aproximación al delito informático", en MIR PUIG, S. (Comp.) y VVAA, *Delincuencia informática*, ed. Promociones y Publicaciones Universitarias, Barcelona, 1992, p. 66.

[45] COLÁS TURÉGANO, A., "El delito de instrusismo informático tras la reforma del CP español de 2015", en *Revista Boliviana de Derecho*, nº 21, enero 2016, p. 212, disponible en

ciberdelitos como "*conductas unidas por el denominador común de ser realizadas mediante las nuevas tecnologías*".

Por tanto, ante la falta de referencia del legislador, será el intérprete quien determine en cada caso si nos encontramos ante un supuesto de delincuencia informática atendiendo en numerosas ocasiones a las complejidades tecnológicas y a normas civiles y administrativas, con los consiguientes riesgos para uno de los principios informadores del Derecho penal como es el principio de legalidad.

Pues bien, en este contexto aparece la figura del *hacking*, considerado el más fulgurante de los delitos informáticos[46], con unas estadísticas que se cuentan anualmente por millones a nivel mundial[47], aunque en nuestro país se han contabilizado 220 procedimientos judiciales relacionados con los ataques a sistemas informáticos[48].

---

http://www.scielo.org.bo/pdf/rbd/n21/n21_a10.pdf, consultado el 18 de septiembre de 2016.

[46] LÍBANO MANZUR, C., "Los Delitos de Hacking en sus Diversas Manifestaciones", en *REDI Revista Electrónica de Derecho Informático*, nº 21, abril 2000, p. 2.

[47] Así, la compañía Kaspersky ha publicado unas estadísticas de 758.044.650 ataques maliciosos contados en 212 países y neutralizados por sus productos. Estadísticas disponibles en https://go.kaspersky.com/LATAM_Security_Bulletin_2016_Stats_SP_SOC_2016.html consultado el 5 de enero de 2017.

[48] Según la Memoria de la Fiscalía General del Estado correspondiente al año 2016, entre los delitos informáticos se contabilizan 22.575 procedimientos judiciales, de los cuales 220 se corresponden a los delitos de ataques o interceptación de sistemas y datos previstos en los artículos

### *1.3 Rasgos de la delincuencia informática.*

Partiendo de las premisas expuestas en el apartado anterior, los delitos informáticos en general, la criminalidad o delincuencia informática se presentan como un fenómeno donde, tal y como indica MIRÓ LLINARES[49], no existe un bien jurídico común afectado, sino que en realidad podemos referirnos a una zona de riesgo que resulta de la generalización de las nuevas tecnologías y que es común a muchos bienes jurídicos protegidos. Por tanto, el primer rasgo es el peligro para los bienes jurídicos más importantes como consecuencia de la aparición de esos nuevos intereses y formas de comunicación. Se trata de una categoría de conductas y no necesariamente de tipos penales.

A ello se añade, como segunda característica, la mayor sencillez para llevar a cabo estos comportamientos, señalado por BARRIO ANDRÉS[50], en la medida que procesalmente las pruebas no son contundentes y pueden verse manipuladas con facilidad, concurre especial lentitud en la investigación de los hechos, favoreciendo su

---

197 *bis* y *ter* CP, p. 601. Memoria disponible en https://www.fiscal.es/fiscal/publico/ciudadano/documentos/memorias_fiscalia_general_estado/!ut/p/a1/04_Sj9CPykssy0xPLMnMz0vMAfGjzOI9HT0cDT2DDbwsgozNDBwtjNycnDx8jAwszIAKIpEVuPtYuBk4unsGO5l6eBhbBJkQp98AB3A0IKQ_XD8KVYm_h68R0AWGvqEmli7GBu6G6AqwOBGsAI8bCnJDIwwyPRUByaZ9lg!!/dl5/d5/L2dJQSEvUUt3QS80SmlFL1o2X0lBSEExSVMwSjhSMzYwQTgyRkJCSEwyMDg2/?selAnio=2016, consultado el 5 de enero de 2017.

49 MIRÓ LLINARES, F., *El Cibercrimen …*, *cit*., nota 8, p. 36 y 27.

50 BARRIO ANDRÉS, M., "El régimen jurídico de los delitos …", *cit*., nota 23, p. 35.

obstaculización o destrucción de pruebas, y puede concurrir cierto anonimato o enmascaramiento del autor, que puede emplear personalidades ficticias, dificultando así su identificación. Por ello, muchas de estas conductas no se descubren o son descubiertas tarde, produciéndose lo que el citado autor denomina "macro-victimización".

En línea con este segundo rasgo citado, la Fiscalía General del Estado se refiere en su Memoria del año 2016[51] a la dificultad para determinar la cifra de delincuencia informática "*dada la escasa frecuencia con la que los afectados/perjudicados comunican el ataque del que han sido víctimas a las fuerzas policiales y/o a los órganos de la Administración de Justicia*". Y explica esta circunstancia por varios motivos: (i) "*la falta de conciencia del carácter delictivo de la conducta*"; (ii) "*cierto factor de desconfianza en las capacidades de actuación frente a estas acciones*"; y (iii) "*razones de carácter reputacional cuando el conocimiento público del hecho pueda afectar al prestigio de empresas y/o instituciones públicas o privadas*". Si bien señala un progreso lento en el cambio de actitud al tomarse "*una mayor conciencia de la ilicitud de estas conductas y de la necesidad de ofrecer respuestas efectivas a partir de los mecanismos del Estado de Derecho*".

En la citada Memoria, también se destaca como característica de este fenómeno "*que se desarrolla en el ciberespacio, más allá de límites territoriales y fronterizos y cuyos artífices se sirven de las*

[51] Memoria, *cit*., nota 48, p. XXI.

*diferencias en los ordenamientos jurídicos nacionales para dificultar su persecución y sanción y, en definitiva, procurar su impunidad*"[52].

Por su parte, DÍAZ MARTÍNEZ[53] enumera los factores que favorecen el auge de la delincuencia tecnológica: (i) la ausencia de inmediación entre autor y víctima; (ii) la despersonalización de la conducta cuando se actúa en el ciberespacio, produciéndose una especie de anestesia en la relación causa-efecto; (iii) la tecnología se convierte en un instrumento que facilita la ocultación de los rastros del delito; (iv) cierta ausencia de normas, tanto en la conciencia del sujeto que lleva a cabo estas conductas, que cree que actúa en un sitio ajeno al Derecho, como en la realidad por no existir un ordenamiento consolidado y eficaz que regule el ciberespacio; (v) la extraterritorialidad de las acciones, con los consiguientes problemas para su persecución.

Por último, MENÉNDEZ MATO y GAYO SANTA CECILIA[54] destacan la dificultad para el descubrimiento, persecución y prueba de estas conductas, motivada por la vulnerabilidad de los equipos y sistemas informáticos y la especialización en los sujetos que las llevan a cabo.

Por todo ello, podemos concluir que en las conductas de

---

52 *Ibíd*., p. 591.

53 DÍAZ MARTÍNEZ, M., "El factor criminógeno de las TIC", en PÉREZ GIL, J. y VVAA, *El proceso penal en la sociedad de la información*, ed. La Ley, Madrid, 2012, p. 534-538.

54 MENÉNDEZ MATO, J. C. y GAYO SANTA CECILIA, M. A., *Derecho e informática ..., cit*., nota 26, p. 319.

*hacking* a las que se refiere el presente trabajo concurren las características propias de la delincuencia informática, siendo por tanto parte del citado fenómeno. Así, en resumen:

1. Concurre una zona de riesgo que resulta de la generalización de las nuevas tecnologías y que es común a muchos bienes jurídicos protegidos. Con el acceso ilícito a los sistemas informáticos se produce un peligro para los intereses más importantes, incluyendo bienes de nueva aparición con el desarrollo de la informática.
2. Existe cierta sencillez para llevar a cabo estos comportamientos, donde el acceso remoto a un sistema informático puede dejar poco rastro del acceso, con las consecuentes dificultades para su persecución y castigo, y puede concurrir cierto anonimato del autor.
3. El citado acceso remoto también permite que las conductas puedan llevarse a cabo sin límites fronterizos, facilitando su impunidad.
4. La ausencia de inmediación autor-víctima, despersonalización, la tecnología al servicio de facilitar la impunidad de la conducta, la inexistencia de un ordenamiento supranacional suficientemente consolidado y eficaz, han determinado un auge de estas conductas que ha exigido la reforma en nuestro Código Penal con las LO 5/2010 y 1/2015.
5. El acceso ilícito requiere de cierta vulnerabilidad de los

equipos y sistemas informáticos y la especialización en los sujetos que las llevan a cabo.

En consecuencia, nos encontramos ante parte del fenómeno de la criminalidad informática, que ha tenido una evolución que a grandes rasgos se expone a continuación.

## *2. EVOLUCIÓN HISTÓRICA.*

### *2.1 Las primeras manifestaciones.*

Una de las razones por las cuales el fenómeno *hacking* sigue siendo un reto para los operadores jurídicos es el desarrollo técnico constante y el continuo cambio en las formas de llevar a cabo estas conductas[55]. El intercambio de información a través de Internet y las nuevas tecnologías conlleva numerosas ventajas, pero también potenciales peligros para los ciudadanos y la sociedad en general, entendida ahora como una sociedad de la información. Por definición, el citado fenómeno está vinculado a estas nuevas tecnologías, siendo en este ámbito donde ha aparecido y se ha desarrollado en los últimos cincuenta años. En síntesis, es posible marcar las siguientes pautas atendidos los ciberataques registrados en estos años:

[55] GERCKE, M., "Comprensión del Ciberdelito. Fenómenos, dificultades y respuesta jurídica", en *International Telecommunication Union*, septiembre 2012, p. 14, consultado el 14 de septiembre de 2016 en http://www.itu.int/en/ITU-D/Cybersecurity/Documents/CybcrimeS.pdf.

Sin perjuicio de que algunos autores se han referido a los chicos despedidos por la Compañía de telégrafos Bell en 1878[56] como *proto-hackers*[57], generalmente los inicios del *hacking* se ubican en torno a 1959, cuando un grupo de especialistas desarrollaron programas para neutralizar otros dentro del mismo sistema. Eran usuarios que no buscaban hacer daño intencionado, modificando lo estrictamente necesario en los sistemas informáticos, sin ánimo de lucro ni de venganza. Su finalidad era esquivar la seguridad de los sistemas. De esta forma, se entiende que los primeros pasos de la ciberdelincuencia fueran en los años 60, con la aparición de los sistemas informáticos basados en transistores y la difusión de estas nuevas tecnologías, enfocándose en los daños a las redes telefónicas de larga distancia, los sistemas y datos informáticos. Puesto que estas nuevas tecnologías no eran accesibles para todas las personas sino que se ubicaban en el ámbito institucional y empresarial, los primeros ciberdelincuentes solían ser funcionarios o empleados descontentos.

Por tanto, en esta época estas conductas son una modalidad de delito contra la propiedad que todavía perdura en la actualidad como una de las formas de delincuencia informática más extendidas,

---

[56] STERLING, B., "The hacker crackdown: law and disorder on the electronic frontier", en *Literary Freeware*, 1992, consultado el 14 de septiembre de 2016 en http://web.mit.edu/hacker/part2.html.

[57] El término *proto-hacker* está actualmente asociado a personas que aspiran a ser *hackers*, pero aún no han adquirido las habilidades necesarias para conseguirlo sin activar los sistemas de alarma. En este sentido, http://www.yourwindow.to/information-security/gl_hacker.htm, consultado el 14 de septiembre de 2016.

existiendo informes de daños causados intencionadamente incluso por los propietarios de los ordenadores dañados[58].

Constituye un ejemplo de este tipo de comportamientos el incendio en 1969 en la Universidad Sir George Williams (Canadá) como consecuencia de una revuelta estudiantil que causó la destrucción de los datos informáticos allí almacenados. El origen de este caso se encuentra en la acusación de racismo a un profesor por parte de seis estudiantes antillanos en 1968. Aunque se creó un Comité para investigar las acusaciones, surgieron problemas con las nominaciones de sus miembros. El 29 de enero de 1969 los denunciantes abandonaron las audiencias y ocuparon un edificio universitario, donde amenazaron con destruir los sistemas informáticos si se avisaba a la Policía, tal y como finalmente sucedió, causando un incendio y daños por valor de dos millones de dólares y resultando detenidas 97 personas[59].

Por otro lado, en este período encontramos los primeros accesos a sistemas de seguridad con ánimo de lucro o por venganza, si bien de forma autorizada, así como los primeros ataques a sistemas de telecomunicaciones de larga distancia[60]. También se ubica en 1961 el

---

[58] DELIO, M., "Battered computers – an epidemic", en *Wired News*, 6 de mayo 2001, consultado el 14 de septiembre de 2016 en hhttp://archive.wired.com/culture/lifestyle/news/2001/06/44284?currentPage=all.

[59] La historia del Centro de ordenadores de la conocida hoy como Universidad Concordia está disponible en http://archives.concordia.ca/fr/node/1695, consultado el 14 de septiembre de 2016.

[60] KABAY, M. E., "A brief History of computer crime: an introduction

inicio de la cultura *hacker*[61], cuando el Instituto Tecnológico de Massachusets (MIT) adquirió el ordenador PDP-1, extendiéndose su influencia y argot con la aparición de la citada ARPANET a partir de 1969, que permitió el intercambio de información entre esta nueva tribu en la red[62].

En esta década comienza a cuestionarse en Estados Unidos la conveniencia de que se hubiese creado una unidad central para almacenar los datos de los distintos ministerios, con los consiguientes abusos y peligros derivados del acceso no autorizado a esos datos, que estaban vinculados a la privacidad. Uno de los primeros autores en advertir sobre el tratamiento informático de los datos personales y su posible uso conjunto fue MILLER[63]. Surge en este ámbito la tutela de

---

for students", en *School of Graduate Studies*, 2008, p. 4, consultado el 14 de septiembre de 2016 en http://www.mekabay.com/overviews/history.pdf.

[61] LEVY, S., *Hacker*, Ed. O'Reilly, Sebastopol (California), mayo de 2010, p. 41.

[62] RAYMOND, E. S., "A brief History of Hackerdom", en *Eric's random writings*, consultado el 14 de septiembre de 2016 en http://catb.org/esr/writings/hacker-history/hacker-history.html#toc3.

[63] Entre las obras de este prolífico autor destaca por su fecha y carácter visionario la dedicada a la *privacy* y el centro nacional de datos, MILLER, A.R., "The national data center and personal privacy", en *The Atlantic*, noviembre de 1967, donde se presenta al ordenador como mucho más que una máquina de sumar o biblioteca en miniatura, haciendo referencia a los sistemas informáticos unidos en el futuro a satélites con un gran intercambio de información. El autor destaca los beneficios, p. ej., en el campo de la medicina, pero también advierte sobre los riesgos por la creación del Centro Nacional de Datos. Este ordenador puede convertirse en un sistema de vigilancia del gobierno que va a suponer la ruptura entre los sistemas estadísticos y los de inteligencia, razón por la cual propone la creación de una estructura jurídica adecuada para evitar el mal uso de la información. Disponible en http://blog.modernmechanix.com/the-national-

la *privacy*, que supera el tradicional derecho a la intimidad para referirse a la acumulación y al uso que puede realizarse de los datos personales. La *privacy* sería primero amparada en el ámbito civil y administrativo y, después, en el ámbito penal, tal y como veremos más adelante.

En los años 70 el incremento de los sistemas informáticos y el almacenamiento de los datos es un fenómeno notable, variando las estimaciones en torno al número de ordenadores en cada país pero apreciándose unas cifras cercanas a los 100.000 en ordenadores centrales y el doble en ordenadores personales sólo en Estados Unidos[64].

Los ordenadores expanden su mercado llegando al público en general como consecuencia de su abaratamiento. Esta expansión conlleva nuevas formas de ciberdelincuencia, ya no sólo centradas en los delitos contra la propiedad sino también en la manipulación de datos, apareciendo un nuevo tipo de delitos: los fraudes informáticos, de naturaleza económica, promediando unas pérdidas en Estados Unidos de 10 millones de dólares al año en el período de 1973 a 1977[65].

---

data-center-and-personal-privacy/, consultado el 14 de septiembre de 2016.

[64] VOLGYES, M. R., "The investigation, prosecution, and prevention of computer crime: a state-of-the-art review", en *The John Marshall Journal of Information Technology & Privacy Law*, 1980, p. 386, consultado el 14 de septiembre de 2016 en http://repository.jmls.edu/cgi/viewcontent.cgi?article=1607&context=jitpl.

[65] HUBBELL NYCUM, S., "Legal problems of computer abuse", en

Los fraudes informáticos, la manipulación de facturas y sueldos en el ámbito industrial y las manipulaciones de saldos en cuentas bancarias han sido desde entonces y hasta la actualidad los ilícitos predominantes[66].

Esta nueva modalidad de delitos supuso un desafío para los legisladores, por cuanto la normativa vigente no contenía una respuesta satisfactoria para estas conductas. En el año 1977, buscando una solución al creciente problema, Estados Unidos elaboró un Proyecto de Ley para regular como delito el uso, para fines fraudulentos o ilegales, de ordenadores de los Estados Unidos, ciertas instituciones financieras y que afecten al comercio internacional[67].

---

*Washington University Law Reviex*, 1977, p. 527, consultado el 14 de septiembre de 2016 en http://openscholarship.wustl.edu/cgi/viewcontent.cgi?article=2611&context=law_lawreview.

[66] SIEBER, U., "Legal aspects computer-related crime – COMCRIME-Study prepared for the European Commission", *University of Würzburg*, 1 de enero de 1998, p. 51, citando el ejemplo de Alemania en 1974, donde se llevaron a cabo manipulaciones salariales por un programador alterando los programas de contabilidad y balance de la empresa con un programa específico para este fin defraudatorio. El defraudador llevó a cabo la creación de trabajadores ficticios en las bases de datos de la empresa y estableció su propia cuenta bancaria como destino de los salarios ficticios, llegando a defraudar el equivalente a 98.679 €. En el mismo año y país, también se cita el ejemplo del German Herstatt Bank, donde la manipulación se produjo en el teclado del ordenador para acceder al negocio bancario, llegando a alcanzar los mil millones de marcos alemanes defraudados. Disponible en http://www.edc.uoc.gr/~panas/PATRA/sieber.pdf, consultado el 14 de septiembre de 2016.

[67] "Federal Computer System Protection Act of 1977", de fecha 27 de

En la década de 1980 continúa la expansión de los sistemas informáticos, con el consiguiente incremento de potenciales ciberdelincuentes y objetivos de la ciberdelincuencia.

La expansión de los ordenadores conlleva un mayor crecimiento y desarrollo del *software*, apareciendo la piratería de *software* y la vulneración de la propiedad intelectual como conductas predominantes entre los delitos informáticos. Por su parte, la interconexión de sistemas informáticos supone como novedad la posibilidad de acceder remotamente de un ordenador a otro y distribuir virus[68] o *software* dañino entre ellos.

---

junio de 1977, disponible en https://www.congress.gov/search?q=%7B"congress"%3A%5B"95"%5D%2C"source"%3A"legislation"%2C"search"%3A"federal+computer+system+protection+act+of+1977"%7D, consultado el 14 de septiembre de 2016.

[68] Según la definición ofrecida por el Instituto Nacional de Tecnologías de la Comunicación, consultado el 14 de septiembre de 2016 en http://www.inteco.es/glossary/Formacion/Glosario/Virus_Glosario, el virus es un "*Programa diseñado para copiarse y propagarse a sí mismo, normalmente adjuntándose en aplicaciones. Cuando se ejecuta una aplicación infectada, puede infectar otros archivos. Se necesita acción humana para que un virus se propague entre máquinas y sistemas*". Como precedentes a este tipo de conductas, cabe indicar que la posibilidad de crear un virus informático fue apuntada en los estudios de John von Neumann en los años 40, tal y como señala FILIOL, E., *Computer viruses: from theory to applications*, ed. Springer, Rennes, 2005, p. 19. También se ha señalado al virus "*Pervading animal*" como el primer virus en el ordenador Univax 1108 (BAIO, A., "Pervading animal and Elk Cloner", 3 de agosto de 2003, consultado el 14 de septiembre de 2016 en http://waxy.org/2003/08/pervading_anima/). Sin embargo, la primera reacción frente a estos ataques dañinos a mediados de los años 80 fue negar su existencia. Incluso Peter Norton

Constituyen ejemplos de estas conductas la puesta en marcha de las denominadas *logic bombs* (bombas lógicas) o programas creados o modificados para producir determinados resultados inesperados y no consentidos por el usuario del *software* cuando concurre una determinada situación (por ejemplo el encendido del ordenador varias veces), siendo programas independientes, o bien parte de *worms* (gusanos)[69], o bien parte de virus[70]. El denominado virus Jerusalem se considera una *time bomb*, modalidad del *logic bomb* que tiene la peculiaridad de que actúa en un momento

---

manifestó que eran un mito urbano como los cocodrilos en las alcantarillas de Nueva York, precisamente quien en 1990 vendería Norton Antivirus como marca propia. En este sentido, DUCKLIN P., "Anti-virus is no good" – discuss", en *nakedsecurity*, http://nakedsecurity.sophos.com/anti-virus-is-no-good-discuss/, consultado el 14 de septiembre de 2016.

[69] Según la definición de "gusano" que ofrecía el Instituto Nacional de Tecnología de la Comunicación, "*Es un programa similar a un virus que se diferencia de éste en su forma de realizar las infecciones. Mientras que los virus intentan infectar a otros programas copiándose dentro de ellos, los gusanos realizan copias de ellos mismos, infectan a otros ordenadores y se propagan automáticamente en una red independientemente de la acción humana*", consultado el 14 de septiembre de 2016 en http://www.inteco.es/glossary/Formacion/Glosario/Gusano_Glosario. El famoso Gusano Morris, o *Morris Worm*, infectó en noviembre de 1988 alrededor de 600 sistemas informáticos, enviando copias y sobresaturando las redes con la consiguiente inutilidad de los sistemas. En este sentido, véase la web de *viruslist*, http://www.viruslist.com/sp/viruses/encyclobrenda?chapter=153311158, consultado el 14 de septiembre de 2016, o más detalladamente, SELTZER, L., "The Morris Worm: Internet malware turns 25", en *Zero Day*, 2 de noviembre de 2013, consultado el 14 de septiembre de 2016 en http://www.zdnet.com/the-morris-worm-internet-malware-turns-25-7000022740/.

[70] KABAY, M. E., "A brief History of computer crime ...", *cit*., nota 60, p. 20.

concreto[71].

En esta época también aparecen los denominados troyanos o *trojan horses*, que son programas aparentemente legítimos pero que están dirigidos a efectuar operaciones no autorizadas por los usuarios, tales como suprimir, bloquear, modificar o copiar datos, o incluso interrumpir el funcionamiento de un ordenador o una red de ordenadores[72]. Al contrario que el virus, el troyano no está dirigido a causar daños ni puede multiplicarse. Fue un ejemplo de troyano en 1982 la manipulación de *software* por parte de los servicios de inteligencia de Estados Unidos cuando la Unión Soviética trataba de adquirir a través de un proveedor canadiense los códigos necesarios para poder automatizar la producción y transporte de petróleo y gas.

---

[71] Este virus, cuya aparición se ubica a finales de 1988, se activaba desde enero de 1989 cada viernes y trece, tal y como se recoge en la web de Alerta-antivirus, http://web.archive.org/web/20071005233501/http://alerta-antivirus.red.es/virus/ver_pag.html?tema=V&articulo=4&pagina=3, consultado el 14 de septiembre de 2016.

[72] Definición contenida en la *web Kapersky lab*, http://www.kaspersky.es/internet-security-center/threats/trojans. El Instituto Nacional de Tecnologías de la Comunicación señalaba en su web, http://www.inteco.es/glossary/Formacion/Glosario/Troyano_Glosario, que "*Este tipo de 'malware' carente de la capacidad de autoduplicación requiere del uso de la ingeniería social para obtener un correcto funcionamiento. Ya sea por la confianza en quien entrega el programa a la víctima o por su falta de cautela, la víctima instala un 'software' aparentemente inocuo en su ordenador. Al ejecutarse el software no se evidencian señales de un mal funcionamiento; sin embargo, mientras el usuario realiza tareas habituales en su ordenador, el programa abre diversos puertos de comunicaciones del equipo de la víctima que permiten el control absoluto de forma remota",* consultado el 3 de junio de 2014.

En ese *software* fue incluido un troyano programado para dejar de funcionar transcurrido un tiempo y haciendo funcionar a altas presiones las válvulas, todo ello con el fin de perjudicar las ganancias y economía soviética[73].

En relación con estas conductas, se ha venido hablando de distintos grupos en el mundo del *hacking*: los sombreros negros, para hacer referencia a los *hackers* que acceden a un sistema informático ajeno con indiferencia ante la ley, valiéndose de las vulnerabilidades en su propio beneficio; los sombreros blancos, que detectan los fallos de los sistemas informáticos e informan al distribuidor del producto para que aplique el parche correspondiente; y los sombreros grises, que se ubican entre los dos grupos anteriores, detectan la vulnerabilidad, avisan a la comunidad *hacker* y a los distribuidores del producto y observan las consecuencias[74].

En definitiva, conforme se incrementó el uso de Internet, también aumentó el acceso no autorizado a los sistemas informáticos que contaban en esta época con escasas medidas de seguridad. Internet era todavía muy joven, prácticamente reducida al ámbito de la ingeniería, militar y profesorado.

---

[73] CASTRO, F., "Mentiras deliberadas, muertes extrañas y agresión a la economía mundial", en *Diario Granma*, 18 de septiembre de 2007, consultado el 14 de septiembre de 2016 en http://www.granma.cu/granmad/secciones/reflexiones/esp-049.html.

[74] CLIFF, A., "Intrusion detection systems terminology", en *Symantec.com*, 3 de julio de 2001, consultado el 14 de septiembre de 2016 en http://www.symantec.com/connect/articles/intrusion-detection-systems-terminology-part-one-h.

En consecuencia, se crearon grupos de estudio en el ámbito de la OCDE[75] y el Consejo de Europa para intentar dar respuesta legal a este fenómeno. En el primero de ellos surgieron unas directrices para la protección de la privacidad y los flujos transfronterizos de los datos personales, tanto públicos como privados, en la medida en que ponen en riesgo la intimidad de las personas. Como principios establecía la limitación en la recogida de datos personales, calidad de los datos, especificación de los fines, limitación de uso, seguridad, acceso a los datos propios y rendición de cuentas[76]. Por su parte, en el Consejo de Europa se suscribe el Convenio para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal el 28 de enero de 1981[77], estableciendo como principios los de compromiso de los Estados firmantes, calidad de los datos, garantías para datos sensibles, seguridad y garantías de acceso.

---

[75] La OCDE, OECD ("*Organization for Economic Cooperation and Development*" en inglés).

[76] La "Recommendation of the Council concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data", de en fecha 23 de septiembre de 1980 – C(80) 58/FINAL, enmendada en fecha 11 de julio de 2013, está disponible en http://acts.oecd.org/Instruments/ShowInstrumentView.aspx?InstrumentID=114&InstrumentPID=312&Lang=en&Book=False, consultado el 7 de enero de 2017.

[77] Convenio disponible en https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016806c1abd, consultado el 7 de enero de 2017.

### *2.2 La expansión del uso de Internet.*

En los años 90 la llegada de Internet para el público en general supuso el acceso e intercambio de una cantidad ingente de información prácticamente en cualquier parte del mundo. La información prohibida en un país llegaba vía Internet desde otro país y a una velocidad antes nunca vista. El acceso a pornografía infantil, la apología del racismo o la xenofobia o el terrorismo cibernético no son sino sólo algunos ejemplos de los nuevos peligros que conlleva la nueva ciberdelincuencia. El *hacking* o acceso ilícito a los sistemas informáticos no es una excepción al incremento de estos delitos, desarrollando modalidades como el envío masivo de correos electrónicos no solicitados a particulares, empresas o instituciones con finalidades de todo tipo, que se convirtió en un verdadero problema con la llegada de Internet al público en general[78].

Internet supone la elevación de los delitos informáticos del ámbito local o regional a un nuevo ámbito global, razón por la cual en el seno de la Asamblea General de la ONU fue dictada la Resolución 45/121, de 14 de diciembre de 1990, sobre prevención del crimen y el

[78] Se considera como primer caso grave de *spam* comercial el incidente de los abogados Laurence Canter y su esposa Martha Siegel, anunciando sus servicios en materia de inmigración y amparándose en su libertad de expresión para el envío de esos mensajes masivos por Internet. Canter fue el primer abogado inhabilitado por el Tribunal Supremo de Tenessee como consecuencia de la publicidad ilegal en Internet. Más información en CRADDOCK, A., "Spamming Lawyer Disbarred", en *wired.com*, 7 de octubre de 1997, consultado el 14 de septiembre de 2016 en http://archive.wired.com/politics/law/news/1997/07/5060.

tratamiento de los delincuentes[79], donde atendidas las nuevas formas de criminalidad y su carácter transnacional, invita a los Estados miembros a coordinar esfuerzos en la lucha contra la delincuencia; y en 1994 emitió el manual para la prevención y el control de los delitos relacionados con la informática[80] con la finalidad de dar una respuesta en el ámbito jurídico en esta época, atendido el problema internacional planteado porque la legislación no ha podido mantener el ritmo del cambio tecnológico, por cuanto según su punto 6, "*El delito informático es una nueva forma de delito transnacional y para luchar eficazmente contra él se requiere una cooperación internacional concertada*", dedicando sus puntos 74 a 82 al "*acceso no autorizado a servicios y sistemas informáticos*" y repasando los distintos instrumentos internacionales dictados hasta su fecha para armonizar las legislaciones nacionales.

Con el nuevo milenio se fueron perfeccionando las nuevas formas de ciberdelincuencia, a la vez que las tradicionales

---

[79] "Octavo Congreso de las Naciones Unidas sobre Prevención del Delito y Tratamiento del Delincuente, A/RES/45/121", de fecha 14 de diciembre de 1990, disponible en http://www.un.org/documents/ga/res/45/a45r121.htm, consultado el 7 de enero de 2017.

[80] Manual de las Naciones Unidas sobre prevención y control de delitos informáticos, Revista Internacional de Política Criminal, Números 43 y 44, 1994, consultado el 14 de septiembre de 2016 en https://www.google.es/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=0CCkQFjAA&url=https%3A%2F%2Fcms.unov.org%2FDocumentRepositoryIndexer%2FGetDocInOriginalFormat.drsx%3FDocID%3Dd387f5c7-8c0d-41ad-b354-a154c3de1f8d&ei=tMSWU8aJJKWX1AW0rQE&usg=AFQjCNH7Qm-EH-Nw78upQ6fVxKEnCb5CQw&bvm=bv.68445247,d.d2k&cad=rja.

modalidades también incrementaron.

Internet supone un incremento de la ciberdelincuencia tanto en número, como consecuencia de los automatismos, como en sus modalidades. El denominado *phishing*, que podemos entender como "*el intento de obtener información confidencial (contraseñas y datos de tarjetas de crédito, por ejemplo) de manera fraudulenta, usurpando la personalidad de un interlocutor fiable en una comunicación electrónica*"[81], tiene numerosas variantes, como el *pharming*, que siguiendo a FERNÁNDEZ TERUELO podemos concebir como la manipulación de direcciones DNS que utiliza el usuario para dirigirlos a una página distinta a la auténtica, pero con la misma apariencia, para conseguir datos confidenciales, todo ello modificando un pequeño archivo denominados *hosts*[82]; el establecimiento de archivos espías (*spyware*) en el ordenador de la propia víctima para el envío de información a otro sistema informático; o el *child grooming*, entendido como "*las acciones realizadas deliberadamente con el fin de establecer una relación y un control emocional sobre un menor con el fin de preparar el terreno para el abuso sexual del menor"*[83]. Todas estas conductas no son sino

---

81 Definición contenida en la Nota 2 de la Comunicación de la Comisión al Parlamento Europeo, al Consejo y al Comité de las Regiones - Hacia una política general de lucha contra la ciberdelincuencia, COM (2007) 267, *cit*., nota 29.

82 Definición de FERNÁNDEZ TERUELO, J. G., *Derecho penal e internet,* ed. Lex Nova, Valladolid, 2011, p. 38.

83 Definición contenida en el FD 1º de la STS, Sala Segunda, de 24 de febrero de 2015, nº 97/2015, recurso 1774/2014, Pte. Excmo. Sr. D. Juan

algunos ejemplos de nuevas modalidades de delincuencia informática.

Todo ello sitúa la ciberdelincuencia como uno de los principales problemas para los países, organizaciones y ciudadanos, que se encuentran con un ordenamiento que no protege adecuadamente los intereses públicos y privados frente a este nuevo fenómeno que se ve multiplicado por Internet. Actualmente cualquier delito puede cometerse o verse favorecido en su comisión gracias a las nuevas tecnologías e Internet, pensemos en el ejemplo antes expuesto del acceso a un sistema informático hospitalario para alterar la distribución de medicamentos, donde podría llegar a apreciarse una tentativa de asesinato[84], que constituye una modalidad que podría trasladarse a cualquier otro sistema público o privado y relacionarse con cualquier otro bien jurídico protegido.

Por tanto, el ritmo frenético en la aparición de las nuevas tecnologías y el incremento progresivo del *hacking*[85] son una realidad. Precisamente el carácter internacional ha sido el principal motivo de cooperación entre los Estados[86] en materia de ciberdelincuencia en

---

Ramón Berdugo y Gómez de la Torre (EDJ 2015/26815). Se entiende, por el análisis que la Sentencia realiza del artículo 183 *bis*, que la conducta se lleva a cabo "*a través de Internet, del teléfono o de cualquier otra tecnología de la información y la comunicación*".

[84] DE LA MATA BARRANCO, N. J., "Los delitos vinculados a las tecnologías ...", *cit*., nota 28, p. 42.

[85] La Comunidad Anti-hacker *HackerWatch* con la información facilitada por usuarios de todo el mundo recopila los intentos de intrusión atendiendo a la actividad de sus cortafuegos, publicando sus informes de *hacking* en la web http://www.hackerwatch.org

[86] ORTIZ PRADILLO, J. C., "<<Hacking>> legal al servicio de la

general y con el *hacking* en particular.

### *2.3 Evolución normativa en el ámbito supranacional.*

La situación táctica descrita generó la lógica preocupación social. Es por ello que dado que los Estados europeos no han sido ajenos a los riesgos que acompañan a las nuevas tecnologías para los derechos individuales y colectivos, siempre ha existido una tendencia a armonizar las normativas nacionales tanto en el ámbito del Consejo de Europa como en el de la Unión Europea. En síntesis y como más relevantes:

i. Encontramos los orígenes en los años 80 en los grupos de estudio de la OCDE y el Consejo de Europa para intentar dar respuesta legal al acceso no autorizado a sistemas informáticos. En el primero de ellos surgieron unas directrices para la protección de la privacidad y los flujos transfronterizos de los datos personales, tanto públicos como privados, en la medida en que ponen en riesgo la intimidad de las personas. Por su parte, en el Consejo de Europa se suscribe el mencionado Convenio para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal el 28 de enero de 1981.

---

investigación criminal: nuevos instrumentos para la investigación y prueba de la delincuencia informática", en VVAA, *Delincuencia informática. Tiempos de cautela y amparo*, ed. Aranzadi, primera edición, Navarra, 2012, p. 181.

ii. La Asamblea General de la ONU dictó en 1990 la Resolución 45/121, relativa a la prevención del delito y tratamiento del delincuente donde, como ya se ha dicho antes, invitaba a los Estados miembros a coordinar esfuerzos en la lucha contra estas nuevas formas de delincuencia.

iii. El denominado Grupo de Trevi de diciembre de 1991, que aglutinaba a ministros de interior de los distintos estados miembros, fue el encargado de un estudio sobre las telecomunicaciones y la posibilidad de su interceptación[87]. En su Informe se exponía la necesidad de estudiar los efectos de la evolución jurídica en el sector de las telecomunicaciones y las medidas a adoptar para contrarrestar los crecientes problemas en este ámbito, cada vez más evidentes.

iv. La Asamblea General de la ONU dictó en 1994 el mencionado Manual para la prevención y el control de los delitos relacionados con la informática[88].

v. El Consejo de la Unión Europea emitió en fecha 17 de enero de 1995 una Resolución estableciendo instrucciones para la interceptación de las comunicaciones tanto por operadores públicos

---

87 El Informe Statewatch "European Union and FBI launch global surveillance system", disponible en http://cryptome.org/jya/eu-fbi.htm, consultado el 14 de septiembre de 2016. Sobre la evolución del Grupo de Trevi, BUNYAN, T., "Trevi, Europol and the European state", en *Statewatching the new Europe*, 1993, consultado el 14 de septiembre de 2016 en http://www.statewatch.org/news/handbook-trevi.pdf.

88 "Manual de las Naciones Unidas sobre prevención y control de delitos informáticos", *cit.*, nota 80.

como privados[89], estableciendo una serie de requisitos en su Anexo para que las autoridades competentes de los Estados miembros puedan realizar la citada interceptación.

vi. En la Recomendación 95/13 dictada por el Consejo de Europa en fecha de 11 de septiembre de 1995, se pone de manifiesto la falta de regulación en el acceso a los sistemas informáticos y a los datos contenidos en ellos[90]. También establece una serie de principios orientadores para las legislaciones de los Estados miembros en materia de información tecnológica, como son los de separación entre búsqueda e interceptación de sistemas y los datos almacenados en ellos dentro de las leyes penales, la necesaria vigilancia técnica de forma que puedan modificarse las leyes conforme evoluciona la informática, la obligación de cooperar con las autoridades en la investigación de los sistemas, medidas a adoptar respecto a las pruebas electrónicas, evaluación continua de los riesgos de las nuevas tecnologías con respecto a la comisión de delitos, permitiendo a las autoridades elaborar contramedidas adecuadas, y por último la necesaria cooperación internacional para poder extender las búsquedas

---

89 Resolución del Consejo de 17 de enero de 1995 sobre la interceptación legal de las telecomunicaciones, publicada en DOUE nº C 329, de 4 de noviembre de 1996, consultado el 14 de septiembre de 2016 en http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=uriserv:OJ.C_.1996.329.01.0001.01.SPA.

90 "Recommendation No. R (95) 13 of the Committee of Ministers to member states concerning problems of criminal procedural law connected with information technology", consultado el 14 de septiembre de 2016 en http://www.coe.int/t/dghl/standardsetting/media/doc/cm/rec%281995%29013_EN.asp.

a sistemas localizados en jurisdicciones extranjeras.

vii. El estudio sobre los "*Aspectos legales de delincuencia informática en la sociedad de la información – COMCRIME*" elaborado por el Profesor Dr. Ulrich Sieber el 1 de enero de 1998[91] en la Universidad de Wuzburgo para la Comisión Europea. El estudio va dirigido a ayudar a este organismo con información relativa a delitos relacionados con la informática, especialmente en lo que respecta a la ley penal sustantiva, procesal y con la aportación de soluciones alternativas. Para ello el autor expone la vulnerabilidad de la sociedad de la información, la situación legal nacional e internacional, la necesidad de adoptar medidas a nivel internacional contra la delincuencia informática, y realiza específicas recomendaciones a la Unión Europea, tanto extralegales (mejorar la inteligencia en las conexiones entre criminalidad informática y organizaciones criminales, mayor educación en la materia, o códigos de conducta en la industria internacional) como legales (elaboración de una directiva sobre la responsabilidad en el acceso a Internet, la configuración de una lista de actos ilegales para garantizar la seguridad informática, o actualizar una base de datos de delitos informáticos).

viii. La Comunicación de la Comisión al Consejo, Parlamento Europeo, Comité Económico y Social y al Comité de las Regiones, de fecha 26 de enero de 2001, fue emitida por la necesidad de que exista una iniciativa política "*con el fin de mejorar la seguridad de las infraestructuras de información y luchar contra la*

[91] SIEBER, U., "Legal aspects computer-related crime ...", *cit*., nota 66.

*delincuencia informática, de acuerdo con el compromiso de la Unión Europea de respetar los derechos humanos fundamentales*"[92]. Su punto 5.2 está dedicado a la retención de datos sobre tráfico por los Estados miembros para prevenir, investigar o perseguir delitos o utilización no autorizadas de los sistemas de telecomunicaciones, en la medida en que la creciente oferta de los proveedores de servicios de comunicaciones va dirigida a reducir el almacenamiento de datos, puede suponer una reducción de material para la investigación, por lo que se propone porque los proveedores conserven algunos datos durante un mínimo de tiempo, a fin de que puedan posteriormente ser utilizados en la aplicación de la ley. Todo ello, adoptándose medidas adecuadas y proporcionadas conforme al derecho comunitario e internacional, atendida la sensibilidad de la materia concerniente a la retención de datos personales.

ix. El Convenio Europeo sobre la Ciberdelincuencia[93], de fecha 23 de noviembre de 2001, en cuyo Preámbulo se expone "*la necesidad de aplicar, con carácter prioritario, una política penal común con objeto de proteger a la sociedad frente a la ciberdelincuencia, en particular mediante la adopción de una legislación adecuada y la mejora de la cooperación internacional*" y

---

92 El denominado **"**eEurope 2002 COM/2000/0890", disponible en http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:52000DC0890, consultado el 7 de enero de 2017.

93 El Instrumento de ratificación del "Convenio sobre la Ciberdelincuencia" por España, fue publicado en el BOE nº 226, de 17 de septiembre de 2010, disponible en https://www.boe.es/diario_boe/txt.php?id=BOE-A-2010-14221, consultado el 7 de enero de 2017.

al que se hace referencia más adelante, atendida su trascendencia en la regulación del *hacking* en nuestro ordenamiento jurídico interno.

x. La Directiva 2002/58/CE del Parlamento Europeo y del Consejo, de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas[94], que dedica su artículo 4 a la obligación de los proveedores de servicios de comunicaciones electrónicas de adoptar medidas de seguridad de sus servicios y de la red, de tal forma que deberá adoptar técnicas que garanticen una seguridad de sus servicios adecuada al riesgo que exista. Si existe un riesgo específico de que se vulnere la seguridad de la red, el proveedor deberá informar a los abonados sobre el riesgo

xi. La DM 2005/222/JAI, de 24 de febrero de 2005, "*relativa a los ataques contra los sistemas de información*"[95], a la que se hará referencia detallada más adelante atendida su influencia sobre la LO 5/2010 y 1/2015, dirigida a "*reforzar la cooperación entre las autoridades judiciales y otras autoridades competentes, incluida la*

---

[94] La "Directiva 2002/58/CE del Parlamento Europeo y del Consejo, de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas (Directiva sobre la privacidad y las comunicaciones electrónicas)", publicada en el DOUE de 31 de julio de 2002, disponible en http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2002:201:0037:0047:es:PDF, consultado el 7 de enero de 2017.

[95] DM 2005/222/JAI del Consejo, de 24 de febrero de 2005, relativa a los ataques contra los sistemas de información, publicada en el DOUE de 16 de marzo de 2005, disponible en http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2005:069:0067:0071:ES:PDF, consultado el 8 de enero de 2017.

*policía y los demás servicios represivos especializados de los Estados miembros, mediante la aproximación de su legislación penal en materia de ataques contra los sistemas de información*". Esta norma comunitaria impone a cada Estado miembro en su artículo 2, tras exponer varias definiciones, la obligación de adoptar medidas concretas contra el acceso ilegal a los sistemas informáticos.

xii. La Recomendación 2005/10, dictada por el Consejo de Europa en fecha 20 de abril de 2005[96], propone unas medidas de investigación y colaboración en el ámbito internacional incluyendo investigaciones encubiertas. Además, establece como principios generales en la utilización de esas medidas a nivel nacional, la necesaria definición legislativa de las circunstancias y condiciones para el uso de técnicas especiales de investigación, garantizando su uso para una investigación y enjuiciamiento criminal eficiente y sólo en el caso de indicios de delitos graves, la necesaria proporcionalidad entre el uso de esas técnicas y el objetivo, facilitar la tecnología y recursos para el uso de las técnicas especiales de investigación, garantizar la conservación de datos por parte de las empresas de comunicación y los proveedores de telefonía e Internet, y asesorar a las autoridades competentes en el uso de las técnicas especiales de investigación.

xiii. La Directiva 2006/24/CE, del Parlamento Europeo y

[96] "Recommendation Rec (2005) 10 of the Committee of Ministers on "special investigation techniques" in relation to serious crimes including acts of terrorism", disponible en https://wcd.coe.int/ViewDoc.jsp?id=849269&Site=CM, consultado el 7 de enero de 2017.

del Consejo, de 15 de marzo de 2006, sobre la conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones y por la que se modifica la Directiva 2002/58/CE[97]. Según el artículo 1.2 de la Directiva, es aplicable a los datos de tráfico y de localización sobre personas físicas y jurídicas y a los datos relacionados necesarios para identificar al abonado o al usuario registrado, atendiendo de esta forma las indicaciones de la citada Comunicación e-Europe 2002. Su artículo 4 establece la obligación de los Estados miembros de adoptar medidas para garantizar "*que los datos conservados de conformidad con la presente Directiva solamente se proporcionen a las autoridades nacionales competentes, en casos específicos y de conformidad con la legislación nacional",* debiendo cada Estado definir el procedimiento para el acceso a los datos conservados, conforme a los criterios de necesidad y proporcionalidad, atendiendo especialmente la normativa internacional y el CEDH.

xiv. La Comunicación de la Comisión al Parlamento Europeo, al Consejo y al Comité de las Regiones, de fecha 22 de

[97] La Directiva 2006/24/CE del Parlamento Europeo y del Consejo, de 15 de marzo de 2006, sobre la conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones y por la que se modifica la Directiva 2002/58/CE, publicada en el DOUE de 13 de abril de 2006, está disponible en http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:105:0054:0063:ES:PDF, consultado el 7 de enero de 2017.

mayo de 2007[98], que define la ciberdelincuencia en su punto 1.1 como "*actividades delictivas realizadas con ayuda de redes de comunicaciones y sistemas de información electrónicos o contra tales redes y sistemas*", planteando profundizar en la política para combatir esta nueva forma de criminalidad y su evolución, exponiendo los instrumentos jurídicos vigentes y la necesidad de desarrollar instrumentos concretos para luchar contra este creciente fenómeno. En especial, la consolidación de la cooperación entre las autoridades a nivel transfronterizo, la colaboración entre el sector público y privado en los métodos de detección y prevención de los daños causados por esas actividades, atendida la evolución de las tecnologías y su control mayoritario por los operadores privados, y la necesidad de una legislación específica contra la ciberdelincuencia.

xv. La Comunicación de la Comisión al Parlamento Europeo y al Consejo, de fecha 10 de junio de 2009[99], donde tras exponerse los progresos en materia de integración de justicia e interior entre los Estados miembros, se destaca el lento progreso en materia penal, estableciendo entre las prioridades políticas "*Proteger a los ciudadanos*", reforzando la cooperación policial y de justicia penal y se declaran en su punto 2.3 los principios de "*finalidad*,

---

98 "Comunicación "Hacia una política general de lucha contra la ciberdelincuencia", *cit*., nota 29.

99 La "Comunicación "Un espacio de libertad, seguridad y justicia al servicio de los ciudadanos" está disponible en http://www.europarl.europa.eu/intcoop/eurolat/working_group_migration/meetings/27_28_01_2010_brussels/dossier/com%282009%290262_es.pdf, consultado el 8 de enero de 2017.

*proporcionalidad y legitimidad del tratamiento de los datos, duración limitada de conservación, seguridad y confidencialidad, respeto del derecho de las personas y control por una autoridad independiente*". Además, entre otras medidas, propone en su punto 4.3.1 el favorecimiento "*de las políticas que permitan garantizar un nivel muy elevado de seguridad de las redes*", debiendo clarificarse las "*normas de competencia jurisdiccional y el marco jurídico aplicable al ciberespacio para favorecer las investigaciones transfronterizas*".

xvi. El Libro verde sobre la obtención de pruebas en materia penal en otro Estado miembro y sobre la garantía de su admisibilidad, emitido por la Comisión Europea en fecha 11 de noviembre de 2009[100], tiene entre sus fines fomentar la cooperación en la obtención de pruebas entre los Estados miembros. Se considera que las diferencias entre sus sistemas judiciales y la falta de reconocimiento mutuo de sus decisiones, "*no deben dificultar la acción de la justicia en su lucha contra la delincuencia transfronteriza*". Así, se exponen los antecedentes en materia de obtención de pruebas transfronterizas, su admisión en los tribunales y las normas vigentes, y se plantea la consulta de si, tal y como se señala en la citada Comunicación de 10 de junio de 2009, la mejor solución para este problema se encuentra en "*la adopción de medidas comunes sobre la recopilación de pruebas en materia penal*". Para ello se plantean a los Estados miembros una serie de preguntas en materia de obtención y

[100] El denominado Libro verde está disponible en http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2009:0624:FIN:ES:PDF, consultado el 8 de enero de 2017.

admisibilidad de pruebas.

xvii. La Comunicación de la Comisión al Parlamento Europeo, Consejo, Comité Económico y Social Europeo y Comité de las regiones, de fecha 24 de abril de 2010[101], que lleva por título "*Garantizar el espacio de libertad, seguridad y justicia para los ciudadanos europeos*", establece como futuras acciones la iniciativa legislativa para una rápida respuesta a los ciberataques, propuestas legislativas frente a los ataques a los sistemas de información, la creación de una plataforma de alerta europea frente a la ciberdelincuencia, el desarrollo de un modelo europeo para la seguridad informática, las medidas para establecer normas de competencia jurisdiccional en esta materia, así como la ratificación del Convenio sobre ciberdelincuencia de 2001.

xviii. La Directiva 2013/40/UE, de 12 de agosto, "*relativa a los ataques contra los sistemas de información y por la que se sustituye la Decisión marco 2005/222/JAI del Consejo"*[102], dirigida "*a*

---

101 La "Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las regiones" para "Garantizar el espacio de libertad, seguridad y justicia para los ciudadanos europeos - Plan de acción por el que se aplica el programa de Estocolmo", COM (2010) 171 final, está disponible en http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0171:FIN:es:PDF, consultado el 8 de enero de 2017.

102 La Directiva 2013/40/UE del Parlamento Europeo y del Consejo, de 12 de agosto de 2013, relativa a los ataques contra los sistemas de información y por la que se sustituye la Decisión marco 2005/222/JAI del Consejo, publicada en el DOUE el 14 de agosto de 2013, disponible en https://www.boe.es/doue/2013/218/L00008-00014.pdf, consultado el 8 de enero de 2017.

*aproximar las normas de Derecho penal de los Estados miembros en materia de ataques contra los sistemas de información, mediante el establecimiento de normas mínimas relativas a la definición de las infracciones penales y las sanciones aplicables, y mejorar la cooperación entre las autoridades competentes, incluida la policía y los demás servicios especializados encargados de la aplicación de la ley en los Estados miembros, así como los organismos especializados de la Unión, como Eurojust, Europol y su Centro Europeo contra la Ciberdelincuencia y la Agencia Europea de Seguridad de las Redes y de la Información (ENISA)*", que fundamenta la reforma del Código Penal por la LO 1/2015, y a la que se hace referencia en los siguientes apartados.

En consecuencia, la normativa comunitaria no se ha mostrado suficientemente contundente y eficaz en materia de lucha contra el acceso ilícito a los sistemas informáticos, atendida la lentitud y la falta de medios comunitarios para legislar en la materia penal. Esto ha motivado que la respuesta legislativa sea siempre tardía frente a unas conductas que son cada vez más sofisticadas al ritmo que marca el crecimiento acelerado de las nuevas tecnologías. Los principales instrumentos normativos comunitarios, esto es, el Convenio Europeo sobre la Ciberdelincuencia, la DM 2005/222/JAI y la Directiva 2013/40/UE son los que han motivado las únicas reformas en el Código penal español, que como veremos se inician en el año 2010 con la LO 5/2010, en un momento en el que el fenómeno se encontraba en pleno desarrollo desde años antes con la generalización del uso de Internet.

En definitiva, se observa una evolución del fenómeno *hacking* paralela al desarrollo continuo de las nuevas tecnologías, lo que a la vez conlleva un incremento en la preocupación de los Estados por salvaguardar sus propios intereses y los de sus ciudadanos. Pero la respuesta legislativa es lenta y actualmente el problema está todavía lejos de una solución satisfactoria, por cuanto evoluciona y se hace más complejo a la par que Internet alcanza nuevos usuarios y nuevos dispositivos de acceso.

## *3. CONCEPTO DE HACKING.*

Antes de analizar los elementos típicos de la conducta de *hacking*, y una vez expuesto el marco normativo supranacional, conviene realizar una delimitación conceptual del fenómeno.

### *3.1 El concepto sociológico y gramatical.*

Desde el punto de vista meramente gramatical, la RAE define el acceso como "*acción de llegar o acercarse*" o "*entrada o paso*"[103], mientras que en el Diccionario del español jurídico, respecto al término acceder, declara que "*Tratándose de datos, llegar hasta donde se encuentran recogidos o registrados, con la posibilidad de*

[103] Definición disponible en http://lema.rae.es/drae/?val=acceso, consultado el 14 de septiembre de 2016.

*conocerlos o de disponer de ellos*"[104] y, en esta línea, QUERALT JIMÉNEZ[105] entiende que la interpretación debe ser restrictiva, identificando acceder con alcanzar, pero no con obtener, que significa hacerse con el objeto perseguido.

Esta concepción parece ser el punto de partida para el legislador con la reforma del artículo 197.3 por la LO 5/2010 al hacer referencia a la persona que *"acceda"* y con ella, siguiendo a SALVADORI, podemos decir que el legislador crea una figura *ad hoc* para los casos de *hacking* y el *cracking*, cubriendo así las lagunas que con anterioridad a la reforma impedían su castigo[106].

En este sentido, antes de su tipificación, el *hacking* ya había sido definido en el ámbito jurisdiccional por el Juzgado de lo Penal 2 de Barcelona, en su Sentencia de 28 de mayo de 1999, como "*un conjunto de comportamientos de acceso o interferencia no autorizados a un sistema informático o red de comunicación*

---

104 MUÑOZ MACHADO, S. (Dir.) y VVAA, *Diccionario del español jurídico*, ed. Espasa, primera edición, Barcelona, 2016, p. 17.

105 QUERALT JIMÉNEZ, J. J., *Derecho penal español ...*, *cit*., nota 11, p. 340.

106 SALVADORI, I., "Los nuevos delitos informáticos introducidos en el Código penal español con la Ley Orgánica 5/2010. Perspectiva de derecho comparado", en *ADPCP*, ed. Ministerio de Justicia (Centro de publicaciones) y Agencia Estatal Boletín Oficial del Estado, vol. LXIV, 2011, p. 230, consultado el 14 de septiembre de 2016 en https://www.boe.es/publicaciones/anuarios_derecho/abrir_pdf.php?id=ANU-P-2011-10022100252_ANUARIO_DE_DERECHO_PENAL_Y_CIENCIAS_PENALES_Los_nuevos_delitos_inform%E1ticos_introducidos_en_el_C%F3digo_Penal_espa%F1ol_con_la_Ley_Org%E1nica_5/2010._Perspectiva_de_derecho_comparado.

*electrónica de datos, y a la utilización de los mismos sin autorización o más allá de lo autorizado*"[107].

En la misma línea, MIRÓ LLINARES entiende el *hacking* como cualquier conducta por la cual un sujeto accede a un sistema o equipo informático sin autorización del titular del mismo de una forma tal que tiene capacidad potencial para conseguir a cualquier tipo de información que esté en el sistema[108] y MUÑOZ CONDE también ha definido el *hacking* como el acceso, a través de sofisticadas técnicas, a la privacidad de los datos guardados en los sistemas informáticos[109].

Ahora bien, en un sentido estricto, atendiendo a la evolución histórica del fenómeno al que se ha hecho referencia en el punto anterior, podemos entender que el *hacking* es el equivalente al intrusismo informático o violación de una esfera de exclusividad del titular del sistema, con independencia del contenido de ese sistema, donde el propósito del *hacker* es el mero acceso al sistema o datos informáticos. En este sentido, en nuestro ámbito podemos referirnos a estos sujetos como "*persona experta en alguna rama tecnológica que accede a un sistema informático o a informaciones ubicadas en dicho sistema o en la red de telecomunicaciones (bases de datos, programas informáticos, etc.) sin permiso del titular y sin necesidad de móvil o*

---

107 Sentencia del Juzgado de lo Penal 2 de Barcelona, de 28 de mayo de 1999, *cit*., nota 15, FD 1º.

108 MIRÓ LLINARES, F., "Los Delitos Informáticos", en ORTIZ DE URBINA GIMENO, Í. (Coord.) y VVAA, *Memento experto. Reforma penal 2010. Ley Orgánica 5/2010*, ed. Francis Lefebvre, Madrid, 2010, p. 145.

109 MUÑOZ CONDE, F., *Derecho Penal. Parte Especial*, ed. Tirant Lo Blanch, Valencia, 2010, p. 277.

*acción posterior alguna*"[110], hablándose en estos casos de *hacking* blanco en contraposición a la modalidad de *cracking*, donde el propósito del *cracker* es el acceso al sistema para causar un daño sobre el sistema o a su titular al adquirir, modificar o eliminar información[111]. Así, ORTS BERENGUER y ROIG TORRES definen a los *hackers* como aquellas personas expertas en informática que entran en otras máquinas por motivos meramente educativos o de diversión, mientras los *crackers* serían los intrusos con intenciones criminales o vandálicas[112].

Por otra parte, junto a los *hackers*, encontramos a los citados *crackers*, que tenían intención de destruir o lucrarse, los *phreackers*, cuya herramienta eran los sistemas telefónicos, interceptando llamadas o realizándolas sin que el verdadero titular tenga conocimiento de ello y actuando contra las grandes multinacionales y sin ánimo de lucro; o los *viruckers*, que actúan sobre los sistemas informáticos para introducir los virus, con el objetivo de dañar la información almacenada en aquél y que pueden ser de dos tipos: benignos (que no causan daño pero perturban el normal funcionamiento del sistema) y malignos (que dañan el sistema o su información)[113].

---

110 Definición contenida en MUÑOZ MACHADO, S. (Dir.) y VVAA, *Diccionario del español jurídico ..., cit*., nota 104, p. 880.

111 MIRÓ LLINARES, F., *El Cibercrimen ..., cit*., nota 8, p. 54.

112 ORTS BERENGUER, E. y ROIG TORRES, M., *Delitos informáticos y delitos comunes cometidos a través de la informática,* ed. Tirant Lo Blanch, Valencia, 2001, p. 178.

113 Respecto a estas distinciones, DE LA CUESTA ARZAMENDI, J. L. y PÉREZ MACHÍO, A. I., "Ciberdelincuentes ...", *cit*., nota 33, pp. 103-108.

En esta línea, la Sentencia del Juzgado de lo Penal 2 de Badajoz, de 15 de febrero de 2006[114], establecía la distinción entre *hacker* y *cracker* en el FJ Segundo, "*un «Hacker» o persona que utiliza determinadas técnicas para acceder sin la debida autorización a sistemas informáticos ajenos, o dicho en castellano, nos encontraríamos ante un intruso, figura diferente a la del «cracker» o pirata virtual que de manera intencionada se dedica a eliminar o borrar ficheros, a romper los sistemas informáticos y a introducir Virus"* (sic), de esta forma, sigue diciendo la Sentencia que *"la conducta del hacker está guiada por un deseo de vencer el reto intelectual de saltar las barreras del sistema. Tratan de vencer a las claves informáticas de los accesos, de descubrir en suma las lagunas de la protección. Por ello no es de extrañar que muchas compañías los contraten para que, antes de instalar sus sistemas informáticos, analicen si éstos presentan grietas por las que se puede alguien colar en ellas. Como señala González Rus, su éxito presupone que se hayan burlado los medios de seguridad (contraseñas, claves de acceso, passwords), que están ahí colocados para impedirlo y que ponen de manifiesto la voluntad del titular de que la información que se contiene en los mismos no sea conocida más que por quienes están autorizados a ello".*

En consecuencia, la conducta del *hacker* puede estar simplemente orientada a saltar las barreras de un sistema informático,

[114] Sentencia del Juzgado de lo Penal 2 de Badajoz, de 15 de febrero de 2006, núm. 42/2006, Pte. Ilmo. Sr. D. Emilio Francisco Serrano Molera (ARP 2006\46).

descubrir, en suma, las lagunas de protección[115], lo que ha supuesto una forzosa evolución acelerada en sus medidas de salvaguarda.

La aparición de Internet ha traído una nueva vía de actuación con inmensas posibilidades para los *hackers*, que a su vez se puede considerar el punto final del *hacking* blanco, por cuanto la mayoría de países que han legislado en materia de cibercriminalidad han incluido la sanción de las conductas de *hacking*. Sin ir más lejos, todos los países de la Unión Europea han tipificado en mayor o menor medida estas conductas, tal y como se expondrá en el siguiente Capítulo. Los distintos legisladores internacionales han considerado incompatible la existencia de una red de redes abierta y segura para los sistemas en que ella interactúan con la intromisión libre en sistemas ajenos, llegando a concebir que todo acceso no autorizado a los sistemas ajenos debe ser sancionado con independencia de su finalidad.

### *3.2 El concepto normativo.*

En el ámbito normativo, el legislador ha llegado a la concepción de que todo *hacking* es *cracking*, por cuanto es indiferente que el sujeto tenga intención o no de dañar el sistema informático y por tanto se entiende que debe ser castigado, de tal manera que su distinción ha quedado vacía de contenido en el ámbito legal y puede

[115] FERNÁNDEZ TERUELO, J. G., *Derecho penal e internet …*, *cit*., nota 82, p. 96.

llevar a la desaparición de una forma de proceder en Internet que ha sido esencial para la creación y consolidación del sistema[116].

Ésta parece ser la idea introducida con la LO 5/2010 cuando el legislador emplea el término "*acceda*" y con la reforma de la LO 1/2015 "*acceda o facilite a otro el acceso*" para referirse a estas conductas, dando así respuesta al fenómeno *hacking*, que tenía sus primeros pasos en los años 60, tal y como se ha expuesto en el punto anterior.

Estos comportamientos, llevados a cabo por los citados *hackers* con independencia de su finalidad y medios, son encuadrables en el artículo 197.3 CP con la reforma del año 2010 y en su artículo 197 *bis* 1 con la reforma del año 2015.

De todo ello se puede inferir que tampoco normativamente el concepto de acceso va más allá de la genérica entrada en el sistema informático. Siguiendo a JORGE BARREIRO[117], esa acción podrá ser directa, cuando se acceda físicamente al sistema informático ajeno, o remota, en el caso de que el acceso se lleve a cabo por medio de una red informática.

Así pues, el *hacking* comprende también los supuestos más variopintos, desde foros, blogs, chats, administrados por personas

---

116 MIRÓ LLINARES, F., *El Cibercrimen ..., cit*., nota 8, pp. 56-57.

117 JORGE BARREIRO, A., actualizado por GUÉREZ TRICARICO, P. "Delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio", en MOLINA FERNÁNDEZ, F. (Coord.) y VVAA, *Memento práctico penal 2016*, ed. Francis Lefebvre, Madrid, 2015, p. 1041.

físicas o jurídicas, hasta páginas *webs* comprendidas en la *Social Media*[118]. Y resulta indiferente el motivo por el cual se acceda, tal y como veremos, siempre que se lleve a cabo con dolo, conforme resulta de la falta de previsión de un supuesto de acceso imprudente y el tenor del artículo 12 del CP[119]. Y en el concepto normativo resultan igualmente indiferentes los medios empleados para el acceso, por ser un delito de medios indeterminados, siendo de uso común los generadores de claves o *keygens*, así como el empleo de *cracks*, entendidos como programas que realizan una modificación permanente o temporal sobre otro o en su código, para obviar una limitación o candado impuesto a propósito por el programador original[120].

Por último, conviene matizar que el artículo 197 *bis* 1 del CP no se refiere al *hacking* como cualquier acceso a un sistema informático, sino que también requiere de otros requisitos: vulnerar las medidas de seguridad establecidas para impedirlo, ausencia de

---

118 Por *Social Media* se entiende comúnmente el "*conjunto de soportes que permiten enlazar información a través de Internet y que conforman redes sociales y comunidades virtuales. El Social Media nos permite se actores activos o pasivos en la generación de información en Internet"*, conforme a la definición contenida, entre otras, en https://conceptos-redes-sociales.wikispaces.com/Social+media, consultado el 14 de septiembre de 2016.

119 Como sabemos el artículo 12 del CP dispone que "*Las acciones u omisiones imprudentes sólo se castigarán cuando expresamente lo disponga la Ley*".

120 Definición de *crack* generalmente aceptada y contenida en https://es.wikipedia.org/wiki/Crack, consultado el 14 de septiembre de 2016.

autorización y que se acceda al sistema de información o parte del mismo, que serán analizados en el punto dedicado al citado artículo.

A todo el concepto normativo se añade que el legislador español ha optado por reconocer como *hacking* también un segundo grupo de conductas, a las que se refiere en el mismo precepto, es decir, las relativas a la permanencia o mantenimiento en el sistema informático. De tal forma que según la concepción gramatical y sociológica de *hacking* que venimos exponiendo, en un sentido estricto, este segundo grupo no podría entenderse propiamente como un acceso ilícito al sistema informático. Así, en estos casos, gramaticalmente el mantenimiento es el "*efecto de mantener o mantenerse*"[121], es decir, "*proseguir en lo que se está ejecutando*". Se trata como indica SALVADORI[122] de conductas omisivas de parada o permanencia abusiva en el sistema de información. No es propiamente un acceso ilícito. En definición del Diccionario del español jurídico, mantenerse (en morada ajena) supone "*negarse a abandonar la morada de otro a pesar de haber sido requerido para ello por el morador*"[123].

Por tanto, en lo que respecta a la definición normativa, cabe reconocer como conductas de *hacking* también los supuestos de

[121] Definición de la RAE disponible en http://lema.rae.es/drae/?val=acceso, consultado el 14 de septiembre de 2016.

[122] SALVADORI, I., "Los nuevos delitos informáticos ...", *cit*., nota 106, p. 233.

[123] Definición contenida en MUÑOZ MACHADO, S. (Dir.) y VVAA, *Diccionario del español jurídico ...*, *cit*., nota 104, p. 1052.

mantenimiento en el sistema, en la medida en que el legislador incluye estos comportamientos junto al *hacking* y se estudian conjuntamente, incluyéndose como parte del mismo fenómeno. Todo ello a pesar de que, en un sentido estricto, no se trataría propiamente de esta conducta desde el punto gramatical, por cuanto no ha existido un acceso ilícito, sino del mantenimiento en un sistema informático de quien ha accedido lícitamente.

De nuevo podemos concluir que normativamente el concepto de mantenerse no va más allá del concepto genérico, pero el artículo 197 *bis* 1 del CP no se refiere a cualquier mantenimiento, sino que necesita un previo acceso lícito, porque si existe un acceso ilícito nos encontraríamos ante la primera de las conductas, además requiere la voluntad en contra de quien tenga el legítimo derecho a excluirlo, si bien en estos casos no parece necesaria la existencia de medidas de seguridad en el sistema informático, tal y como se expondrá en el Capítulo IV.

En definitiva, un concepto normativo del *hacking* ajustado al artículo 197 *bis* 1 del CP sería el acceso no autorizado a todo o parte de un sistema informático, física o remotamente, con independencia de los medios y finalidad del sujeto, vulnerando las medidas de seguridad establecidas para impedirlo, o bien, tras un previo acceso lícito, la permanencia en todo o parte de un sistema contra la voluntad de quien tenga el legítimo derecho a excluirlo.

## *4. EL HACKING EN EL ORDENAMIENTO PENAL ESPAÑOL.*

### *4.1 La situación antes de la reforma de 2010.*

Tal y se viene exponiendo, en las sociedades informatizadas los datos aparecen organizados en sistemas de almacenamiento y recuperación por lo que, si se quiere evitar su puesta en peligro o lesión, deben estar protegidos frente a accesos no autorizados y destinarse únicamente al fin para el que fueron recabados[124], especialmente cuando se trata de datos personales, por encontrarse amparados bajo el derecho fundamental a la intimidad o la libertad informática.

No es objeto del presente epígrafe la evolución histórica de la tutela de la intimidad, a la que se hace referencia en el punto dedicado al bien jurídico protegido. Sin embargo, en la medida en que el legislador ha optado por incluir las conductas de acceso ilícito a sistemas informáticos entre los delitos contra la intimidad, conviene precisar que actualmente existe un cambio en el entendimiento tradicional del derecho a la intimidad que comprendía el derecho *to be let alone* o de exclusión, surgiendo un nuevo ideal, centrado en el denominado *habeas data* que comprende el control sobre los datos informatizados.

---

[124] GÓMEZ NAVAJAS, J., *La protección de datos ..., cit.*, nota 22, p. 36.

La nueva concepción positiva del derecho a la intimidad no se limita a un mero reconocimiento del derecho por los tribunales, sino que ha venido acompañada de instrumentos de eficacia y aplicación, tanto desde el punto de vista legislativo, con la aprobación de la LO 5/1992 y la posterior LOPD, como desde el punto de vista orgánico, con la creación de organismos encargados de velar por el respeto de estos derechos y las garantías reconocidas en el artículo 18.4 CE y en la LOPD, como es la Agencia Española de Protección de Datos.

Por su parte, con la modificación del artículo 197 operada por la LO 5/2010 en el Código Penal, a la que ha seguido su reforma por la LO 1/2015, por primera vez ya no sólo se tutela en su articulado la libertad informática o *habeas data*, sino que también se regula el mero acceso no autorizado a los sistemas informáticos. De esta forma se produce una tutela anticipada de estos derechos, pues no olvidemos que la ingente utilización de datos personales en la sociedad actual puede hacer muy peligroso su uso, ya no sólo para sus fines comerciales, sino para cualquier otro fin contrario a Derecho, por lo que se hace necesario el establecimiento de límites jurídicos, en mayor medida si consideramos la utilización de datos personales con carácter transfronterizo, lo que implica también la necesidad de soluciones de carácter universal.

Todo ello sin olvidar que, sin perjuicio de la evolución del concepto jurídico de la intimidad, este derecho, como derecho

fundamental, prexiste al nacimiento y al desarrollo de la informática[125] con la consiguiente protección requerida en el ordenamiento jurídico.

Sin embargo, a pesar de que la intimidad ha sido un derecho históricamente tutelado en nuestras legislaciones, lo que posiblemente nos llevaría a remontarnos a la legislación de los pueblos septentrionales y a las denominadas paces perpetuas o la paz del domicilio incluida en la su legislación penal[126], no podemos decir que el *hacking* haya sido tradicionalmente perseguido en nuestro ordenamiento, sin perjuicio de la normativa internacional y comunitaria sobre la materia donde España ha sido Estado parte y a la que nos hemos referido en anteriores apartados. En primer lugar porque, como hemos visto, es un fenómeno por definición asociado a las nuevas tecnologías y, en segundo lugar, porque hasta la reforma del Código Penal en el año 2010 algunas de estas conductas, las más graves, se reconducían a los ataques a la intimidad tutelados en su artículo 197.

El principal problema se daba en el denominado *hacking*

---

125 MARCHENA GÓMEZ, M., "Delitos contra la Intimidad", en DEL MORAL GARCÍA, A., SERRANO BUTRAGUEÑO, I. (Coords.) y VVAA, *Código Penal: Comentarios y Jurisprudencia*, *Tomo II*, ed. Comares de Ciencia Jurídica, Granada, 2001, p. 1526.

126 La paz del domicilio considerada como paz perpetua ha sido mencionada por GUTIÉRREZ FERNÁNDEZ, B., *Examen histórico del Derecho penal*, ed. Analecta, Pamplona, 2003, p. 55. El domicilio se consideraba lugar sagrado posiblemente por la costumbre de colocar símbolos religiosos para la protección de la familia, que luego pasaron a los templos, creando el legislador en el domicilio un espacio de seguridad para los ciudadanos en una época de grandes inseguridades.

blanco o puro, esto es, "*aquellas en las que el intrusismo informático no se encuentra presidido por otro propósito que la demostración de la propia pericia, la superación del desafío que supone la detección de <<agujeros>> de entrada al sistema, etc.*"[127], supuestos en los que, existiendo tan sólo los apartados 1 y 2 del artículo 197 CP, prevalecía la consideración doctrinal de que debían quedar impunes por falta del elemento subjetivo exigido en estos preceptos. Si bien autores como RODRÍGUEZ MOURULLO[128] consideraban necesaria su tipificación como delito autónomo, por cuanto con el acceso ya se había producido una vulneración para la confidencialidad e integridad del sistema informático, otros como MORÓN LERMA[129] o MATA Y MARTÍN[130] entendían preferible su sanción administrativa. Así, según esta última opinión, el mero intrusismo no era contrario a la intimidad informática, porque no suponía un acceso a los datos, sino al sistema informático. Esto suponía que era necesaria la elaboración

---

127 TOMÁS-VALIENTE LANUZA, C., "Título X. Delitos contra la Intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio. Capítulo I. Del descubrimiento y revelación de secretos", en GÓMEZ TOMILLO, M. (Dir.) y VVAA, *Comentarios al Código Penal*, ed. Lex Nova, primera edición, Valladolid, 2010, p. 802.

128 RODRIGUEZ MOURULLO, G., ALONSO GALLO, J., LASCURAÍN SÁNCHEZ, J.A., "Derecho penal e Internet", en CREMADES, J., FERNÁNDEZ-ORDÓÑEZ, M.A., ILLESCAS, R. (Coords.), *Régimen jurídico de Internet*, ed. La Ley, Madrid, 2002, p. 259.

129 MORÓN LERMA, E., *Internet y Derecho Penal ...*, *cit*., nota 5, p. 78.

130 MATA Y MARTÍN, R.M., "La protección penal de datos como tutela de la intimidad de las personas. Intimidad y nuevas tecnologías ", en *Revista penal,* nº 18, consultado el 23 de marzo de 2012 en http://www.uhu.es/revistapenal/index.php/penal/article/viewFile/291/282 , p. 235.

de un nuevo bien jurídico que no podía delimitarse claramente ni tenía cabida en las categorías existentes. Además, se consideraba que, desde el punto de vista del principio de lesividad, no era equiparable a otros delitos informáticos, como los daños informáticos, los supuestos perjuicios económicos por manipulación de sistemas o el acceso o modificación de datos personales. Por último, se hacía referencia a la Recomendación 1989/90, donde no era obligatoria la punición de estas conductas, sino que resultaba opcional su incriminación.

Esta polémica terminaría con la nueva redacción del artículo 197.3 CP por la reforma de la LO 5/2010, aproximadamente reproducido en el nuevo artículo 197 *bis* 1 CP tras la reforma llevada a cabo con la LO 1/2015, con los matices que veremos.

Ahora bien, como hemos anticipado, el hecho de que antes del año 2010 las conductas de intrusismo informático no tuvieran una tipificación específica no suponía que necesariamente pudieran considerarse impunes. Así, cuando este comportamiento era el medio para cometer otra infracción, la sanción de ésta comprendería el *hacking* (por ejemplo, en el caso de la estafa informática del artículo 248.2 CP), que incluso podría ser penado como tentativa en esos supuestos, lo que también pudiera suceder en el acceso no autorizado al sistema informático como medio para atentar contra la intimidad en los casos de los apartados 1[131] ó 2 ("*Las mismas penas se impondrán*

[131] El actual apartado 1 del artículo 197 dispone que "*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*

*al que, sin estar autorizado, se apodere, utilice o modifique, en perjuicio de tercero, datos reservados de carácter personal o familiar de otro que se hallen registrados en ficheros o soportes informáticos, electrónicos o telemáticos, o en cualquier otro tipo de archivo o registro público o privado. Iguales penas se impondrán a quien, sin estar autorizado, acceda por cualquier medio a los mismos y a quien los altere o utilice en perjuicio del titular de los datos o de un tercero*")[132] del artículo 197 CP, relativos, respectivamente, a las

---

*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.*". Este apartado tiene su precedente en el párrafo primero del artículo 497 del Código Penal de 1973, aprobado por Decreto 3096/1973, de 14 de septiembre, por el que se publica el Código Penal, texto refundido conforme a la Ley 44/1971, de 15 de noviembre, donde se establecía que "*El que para descubrir los secretos de otro se apoderase de sus papeles o cartas y divulgare aquéllos será castigado con las penas de arresto mayor y multa de 100.000 a 2.000.000 de pesetas*".

[132] La inclusión de estas conductas comprendidas en el apartado 2 constituye una de las novedades del Código Penal de 1995, superando su consideración como ilícito administrativo. Con anterioridad a 1995 la regulación de esta materia se llevaba a cabo en la Ley Orgánica 5/1992, de 29 de octubre, relativa al Tratamiento Automatizado de Datos de Carácter Personal (BOE nº 262, de 31 de octubre de 1992, disponible en http://www.boe.es/boe/dias/1992/10/31/, consultado el 9 de enero de 2017), que fue sustituida en el ámbito administrativo por la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (BOE nº 298, de 14 de diciembre de 1999, disponible en http://boe.es/boe/dias/1999/12/14/, consultado el 9 de enero de 2017) y que incorporaba como novedad la ampliación del campo de protección de los datos de carácter personal con independencia del soporte en el que se incorporaran.

actividades tendentes al descubrimiento de secretos o vulneración de la intimidad y al apoderamiento, utilización o alteración de datos registrados.

Los órganos jurisdiccionales han dado distintas soluciones al problema. Así, la primera sentencia dictada en España por un caso de *hacking* fue la emitida por el Juzgado de lo Penal 2 de Barcelona en fecha 28 de mayo de 1999 (caso Hispahack)[133], en la que se absolvió al acusado de un delito de daños tipificado en el artículo 264.2 CP por el que el Ministerio Fiscal acusaba a un sujeto por acceder a los sistemas informáticos de una Universidad sin autorización para ello.

En este caso, según constaba en el Atestado de la Guardia Civil, un mensaje de correo electrónico había avisado sobre las actividades de un grupo de *hackers*, adjuntando fotografías de sus integrantes, entre los que se pudo identificar al acusado. Además, con esa información era posible acceder a una página pública ubicada en un proveedor de Internet de Estados Unidos, donde se pretendía que fuese la página de un grupo llamado "Hispahack" y en la que se publicaba un artículo que se atribuía al acusado. De esta forma, fue posible localizar un ordenador a nombre del acusado ubicado en una empresa gibraltareña.

Con estas premisas en cuanto a la regularidad en la investigación, la Sentencia se centraba a continuación en el objeto de

133 Sentencia del Juzgado de lo Penal 2 de Barcelona de fecha 28 de mayo de 1999, *cit*., nota 15.

su enjuiciamiento, es decir, la conducta de intrusismo informático, comenzando por su definición en los términos que se han expuesto en el epígrafe anterior.

La Sentencia consideraba probado el acceso no autorizado a través de Internet a los ordenadores ubicados en las dependencias universitarias en fecha 11 de septiembre de 1997, llegando a obtenerse los privilegios del administrador del sistema en dieciséis máquinas servidoras e instalando programas "*sniffers*" que tenían por finalidad capturar la información que circulaba por la red del sistema. Más concretamente, identificadores y claves de acceso de otros usuarios, enviando los datos obtenidos a través de lnternet a otro ordenador ubicado en un bar, almacenándolos en un directorio correspondiente al usuario "Hispahack".

Sin embargo, aunque el acusado reconocía su pertenencia al citado grupo "Hispahack" y sus iniciales correspondían al usuario y directorio del ordenador ubicado en el bar al que se transfirieron los datos de la Universidad, se consideraba probado pericialmente que el ordenador también tenía utilidades de *hacking* que podían ser utilizadas por cualquiera que accediese al ordenador como usuario del citado grupo, no habiéndose definido el origen de la intrusión. Tan sólo constaba un directorio compartido accesible para cualquier ordenador, sin claves y creado por otras dos máquinas de origen desconocido, sin que en los ficheros existentes en los ordenadores del acusado se evidenciara información sobre esos sistemas. Tampoco estaba acreditado que la persona que instaló los "*sniffers*" fuese la

misma que los usó. Por tanto, no se entendía probado que el acusado participase en esa entrada ilegal, obtención y transferencia de datos informáticos de la Universidad, que había necesitado su reinstalación y que, en definitiva, era la conducta que se le imputaba al acusado, razón por la cual se le absolvió.

El citado caso Hispahack no fue el único donde no se condenaba el acceso a un sistema informático ajeno. Así, en este grupo de casos de absolución encontramos la SAP de Tarragona de fecha 23 de julio de 2001[134]. En ella se consideraba no probado que los acusados tuviesen el *animus desvelandi* de la información obtenida irregularmente, en lo que se definió simplemente como un "*reto personal de obtener información sin fin*" que podríamos encuadrar en una conducta de *hacking*, y por tanto se absolvió a los acusados que habían conseguido los *passwords* del administrador de sistemas informáticos de la Universitat Rovira i Virgili, con los que pudieron capturar los códigos de usuarios y contraseñas que circulaban por esa red. Así, según su FJ Segundo, "*los acusados descubrieron y utilizaron passwords ajenos, accedieron mediante los anteriores a información reservada de terceras personas sin su consentimiento y se les halló herramientas informáticas para causar evidentes perjuicios en programas informáticos y bases de datos",* pero según esta Sentencia, no se podía afirmar que los acusados tuvieran "*ánimo divulgador", "o incluso que poseyendo herramientas para poder*

[134] SAP de Tarragona de fecha 23 de julio de 2001, sec. 2ª, rec. 735/2000. Pte. Ilmo. Sr. D. Nouvilas Puig, Xavier (EDJ 2001/43367 o JUR 2001\310139).

*perjudicar ostensiblemente bases de datos ajenas hayan tenido la intención de usarlas con aquél fin",* considerando más bien *"la actitud de los acusados como un reto personal de obtener información sin fin, esto es, como una voluntad de autocompetición enmarcada en un contexto que vulgarmente podríamos calificar de <<chafarderío informático>>, asimilable al escucha radiofónica que usando un scanner intercepta conversaciones policiales, de navegación aérea etc. con simples fines lúdicos o actuaciones análogas"*.

En el mismo sentido absolutorio también encontramos el Auto del Juzgado de Instrucción 2 de Lorca, de 29 de enero de 2002[135]. Esta resolución declaraba el sobreseimiento libre relativo a un supuesto delito de descubrimiento y revelación de secretos por el intento fallido de acceso a una página ministerial. Después de recordar que las conductas de *hacking* no eran constitutivas de delito, por cuanto en

[135] Auto del Juzgado de Instrucción 2 de Lorca, de 29 de enero de 2002, Procedimiento Abreviado 1527/99, Pte. Sr. D. Antonio Alcazar Fajardo. En este Auto se resolvió el sobreseimiento libre argumentando en su FJ Segundo que "*Este delito* –del 197.1 CP- *ha sido calificado por la doctrina, en cuanto a su naturaleza, como un delito mutilado en dos actos, de tal forma que se realiza una acción como base para un actuar posterior del mismo sujeto activo, produciéndose la consumación tan pronto se realiza la primera acción, integrando la segunda acción el elemento subjetivo del injusto, en este caso, el ánimo de descubrir secretos. 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. En el caso de autos a la duda sobre la finalidad perseguida por D. O. C. cuando supuestamente trató de acceder y copiar los ficheros duda que siempre debe operar <<in dubio pro reo>> se une la falta de acreditación suficiente de que dicho acceso tuviera éxito"*.

ellas se consideraba que sólo existía un ánimo de acceder al *password* pero faltaba el elemento subjetivo del injusto exigido en el primer párrafo del artículo 197 CP, en la Sentencia se declaraba que en este caso se dudaba de la intención del acusado, para lo cual debía acudirse al principio *in dubio pro reo*, y además no estaba acreditado el éxito del acceso, motivando de esta forma el archivo de las actuaciones.

También constituye un ejemplo de fallo donde no hubo condena la STS de 30 de abril de 2007[136], con cita de varias, relativo al acceso de unos miembros del Ayuntamiento de Punta Umbría al ordenador del Gerente de la Sociedad Municipal de Gestión del Suelo, con ocasión de una inspección, en la que uno de esos miembros utiliza la clave de seguridad para acceder al mencionado ordenador, que era de titularidad pública, y al correo electrónico de *Outlook* del Gerente, imprimiendo uno de los mensajes y cotejándolo con los documentos que existían en el Ayuntamiento, supuesto que fue considerado atípico en la mencionada Sentencia a pesar del acceso. Al ser un ordenador de titularidad pública se concluía que no era el lugar adecuado para archivar secretos del querellante por cuanto ese instrumento se consideraba que debía estar al servicio de la función pública, además los acusados accedían circunstancialmente a ese ordenador y, en consecuencia, no era posible resolver que la voluntad de los acusados fuese vulnerar la intimidad del querellante, tal y como se pudo comprobar con su actuación una vez accedieron al ordenador.

---

[136] Sentencia del Tribunal Supremo nº 358/2007, de 30 de abril de 2007, con cita de varias, recurso 1805/2006, Pte. Ilmo. Sr. D. Miguel Colmenero Menéndez de Luarca (RJ 2007\3724).

Más recientemente, el Juzgado de lo Penal número 4 de Alcalá de Henares ha dictado la Sentencia 238/2014, de 24 de junio[137], donde era objeto de enjuiciamiento la conducta por la cual un sujeto había accedido al ordenador de otras personas con capacidad para dañar equipos informáticos en el año 2003. En concreto, la Sentencia absolvía al creador del virus gusano Kelar, acusado porque con el virus infectaba los ordenadores de otros usuarios de Panda, que una vez infectados conectaban con una página que descargaba en los equipos un programa troyano por el que el acusado podía acceder a la información contenida en los ordenadores de las víctimas sin su consentimiento. El acusado fue absuelto de los delitos tipificados en los artículos 197.2 y 264.2 CP. En primer lugar, porque para condenar por el primero de ellos se entendía necesario que el acusado se hubiese apoderado, utilizado o modificado datos reservados de carácter personal o familiar, o accedido, modificado o utilizado esos datos, que no había tenido lugar aunque existía un riesgo potencial de que pudiese llevarse a cabo. Y en segundo lugar, respecto al segundo de los delitos, también concluía esta Sentencia que no se habían producido daños, aunque existía la capacidad de causarlos. Aunque se había producido la ralentización del ordenador de uno de los afectados, no pudo probarse si esta circunstancia era debida a una sobrecarga de información en el ordenador o se debía a otro motivo. No quedaba probada la intención de dañar en el acusado.

[137] Sentencia del Juzgado de lo Penal número 4 de Alcalá de Henares nº 238/2014, de 24 de junio, autos 435/2010, Pte. Dª Nuria Alcalde Alcalde.

Sin embargo, también han existido casos de condena de estas conductas, como el enjuiciado en la Sentencia del Juzgado de lo Penal 2 de Badajoz, de 15 de febrero de 2006, núm. 42/2006[138], donde se defendía la posibilidad de reconducir el *hacking* a los supuestos regulados en el artículo 197 CP. En este caso el acusado fue condenado porque había accedido a los Códigos Binarios de un juego informático de pago y, con ellos, a la disposición absoluta de acceso al mencionado juego, vulnerando las medidas de seguridad establecidas, por un delito de descubrimiento y revelación de secretos del artículo 197.1 CP.

Según la Sentencia, la entonces falta de tipificación del *hacking* en el Código Penal no suponía que los actos concretos de los *hackers* no pudieran acomodarse en alguno de los supuestos encuadrados en artículo 197 CP. Así, si sobrepasando la mera navegación en la red, llegan a descubrir las claves de acceso al sitio, las vulneran y acceden al espacio protegido por la clave, están descubriendo los secretos de otro. Esos comportamientos, logrando quebrantar las claves de acceso a los *passwords*, según el FJ Segundo de la Sentencia, evidencian "*no sólo el dolo genérico de saber lo que se hace y la voluntad de hacerlo sino también el dolo y ánimo especifico requerido por esta figura delictiva, caracterizado por el ánimo tendencial de invadir la esfera de la privacidad que representa precisamente la existencia y colocación de una contraseña de acceso*

[138] Sentencia del Juzgado de lo Penal 2 de Badajoz *cit*., nota 114.

*impeditiva del paso al contenido que hay detrás de la misma."*. Por tanto, concluía que para la consumación del delito era suficiente con la interceptación, *"entendiendo por tal el descubrimiento del password, independientemente del descubrimiento efectivo de la intrusión o secretos ajenos que se esconden detrás de la clave de acceso (que pertenecen a la fase del agotamiento delictual)*".

De esta forma, en el caso enjuiciado el acusado había accedido a la información secreta reservada al titular o administrador del juego y con ella podía utilizarlo y modificarlo, concurriendo las circunstancias del citado artículo 197.1 CP al apoderarse de esas claves o códigos que impedían la entrada, con un acceso inconsentido, alterando su contenido y con la intención de llegar a esos secretos, si bien se le aplicó la circunstancia atenuante analógica de ludopatía, de conformidad con el entonces artículo 21.6ª CP (actual 21.7ª), en relación con lo establecido en el apartado 1 del mismo precepto y en los apartados 1 y 3 del artículo 20 CP[139].

[139] Así, la Sentencia recordaba el criterio jurisprudencial en el que lo trascendente, más allá de si se trata o no de una enfermedad o una forma de neurosis, es la forma en que se manifiesta en cada caso, en cuanto tendencia patológica a jugar y su repercusión en el raciocinio o voluntad del sujeto. En la medida que la compulsión actúa cuando se presenta la oportunidad de jugar, dominando la voluntad hacia el acto de jugar, afectando así a las acciones inmediatamente dirigidas a satisfacer la compulsión. Por el contrario, en los actos más lejanos sólo será un impulso organizado para el futuro placer de jugar, siendo por tanto este último impulso racional y dominable. Por último, serán intrascendentes las acciones ejecutadas con fines distintos al juego. En consecuencia, en el caso concreto, partiendo de que el sujeto cumplía con los criterios para apreciar la patología, y que su actuación fue muy compleja, planeada y reflexiva, se

Por tanto, aunque con anterioridad al 2010 el instrusismo informático podía reconducirse a los tipos previstos para otros delitos informáticos, se observa cómo su castigo era excepcional y la regla general era la absolución por estas conductas.

En cualquier caso, tras la reforma operada por la LO 5/2010, el nuevo artículo 197.3 CP tipificaba expresamente y por primera vez las conductas de *hacking*, señalando en su primer párrafo: "*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".*

Tras la reforma del artículo 197 por la LO 1/2015, las conductas de *hacking* se encuadran en el artículo 197 *bis* CP, en cuyo apartado 1 se establece *"El que por cualquier medio o procedimiento, vulnerando las medidas de seguridad establecidas para impedirlo, y sin estar debidamente autorizado, acceda o facilite a otro el acceso al conjunto o una parte de un sistema de información o se mantenga en*

---

concluía que la circunstancia analógica era simple, porque "*la influencia que sufría le disminuía siquiera sea levemente su libertad y capacidad volitiva*", aplicando el artículo 21.6 (entonces vigente y actual 21.7 "*cualquier otra circunstancia de análoga significación que las anteriores*") en relación con el 21.1 ("*Las causas expresadas en el capítulo anterior, cuando no concurrieren todos los requisitos necesarios para eximir de responsabilidad en sus respectivos casos*") y el artículo 20, apartados 1 (anomalía o alteración física) y 3 (alteraciones en la percepción), del CP.

*él 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".*

Por tanto, el legislador ha optado por castigar cualquier tipo de acceso no autorizado con vulneración de medidas de seguridad, dando cabida tanto a las conductas de *hacking* como los supuestos de *cracking*. Tendremos que esperar a la respuesta de los tribunales para comprobar en la práctica el nivel de exigencia en cada uno de los nuevos elementos del tipo y determinar el bien jurídico para concretar la consumación.

### *4.2 La justificación de las reformas de los años 2010 y 2015.*

#### *4.2.1 La reforma del año 2010.*

Las conductas de *hacking* son tipificadas como novedad en nuestro Código Penal a raíz de la LO 5/2010 y modificadas con la LO 1/2015. Esa primera reforma fue publicada en el BOE de 23 de junio de 2010[140] y supone la vigesimoséptima modificación de su texto.

Una de las novedades introducidas por esta Ley Orgánica fue precisamente la tipificación del acceso a datos o programas contenidos

[140] Disponible en http://www.boe.es/boe/dias/2010/06/23/pdfs/BOE-A-2010-9953.pdf, consultado el 19 de junio de 2014.

en sistemas informáticos o el mantenimiento en estos sistemas, conductas a las que se refiere el presente trabajo. Su justificación se sustenta en la necesaria armonización de la legislación interna con la normativa internacional y en las carencias del Código Penal en materia de delitos informáticos. Es esta la razón que recoge el Preámbulo de la LO 5/2010 cuando afirma que "*para cumplimentar la Decisión Marco 2005/222/JAI, de 24 de febrero de 2005, relativa a los ataques contra los sistemas de información, se ha resuelto incardinar las conductas punibles en dos apartados diferentes, al tratarse de bienes jurídicos diversos*".

Por su parte, la reforma del Código Penal introducida por la LO 1/2015 tuvo su publicación en el BOE de 31 de marzo de 2015[141], y viene motivada igualmente "*para ofrecer respuesta a la delincuencia informática en el sentido de la normativa europea*", llevando a cabo "*la transposición de la Directiva 2013/40/UE, de 12 de agosto, relativa a los ataques contra los sistemas de información y la interceptación de datos electrónicos cuando no se trata de una comunicación personal*", tal y como se expone en el apartado XIII de su Preámbulo y en su Disposición final sexta dedicada a la "*Incorporación de Derecho de la Unión Europea"*.

Una de las peculiaridades del Código español sobre la materia, como señala MORALES GARCÍA[142], es la inexistencia de un Título

[141] Disponible en https://www.boe.es/boe/dias/2015/03/31/pdfs/BOE-A-2015-3439.pdf, consultado el 2 de septiembre de 2015.

[142] MORALES GARCÍA, O., "Delincuencia informática: instrusismo,

específico para los delitos informáticos, de tal forma que esas conductas aparecen reguladas en función de la afectación al bien jurídico.

Tal y como señala el citado Preámbulo de la LO 5/2010, con la reforma se trata de cumplimentar la normativa internacional, en concreto, la DM 2005/222/JAI, introduciendo el cambio por razón del mandato contenido en la normativa europea. No obstante, sobre las conductas de acceso ilícito a los sistemas informáticos, conviene destacar la siguiente normativa previa a la citada Ley Orgánica:

#### *4.2.1.1 El Convenio Europeo sobre Cibercriminalidad.*

En el ámbito europeo, la norma de mayor relevancia es el citado Convenio Europeo sobre Cibercriminalidad, aprobado por el Consejo de Europa el 23 de noviembre de 2001 y suscrito por España el 3 de junio de 2010[143], por cuanto es la primera norma que responde a los ataques criminales contra los sistemas informáticos en este ámbito. Como consecuencia de este Convenio, los Estados miembros se obligan a castigar estas conductas en su ordenamiento penal interno[144]. Tal y como se expone en su Preámbulo, este Convenio se

---

sabotaje informático y uso ilícito de tarjetas", en QUINTERO OLIVARES, G. (Dir.) y VVAA, *La reforma penal de 2010: Análisis y comentarios*, ed. Aranzadi, Navarra, 2010, p. 182.

143 *Cit*., nota 93.

144 Al respecto, el articulo 45 del Convenio establece que "*Solución de*

suscribe con la intención de intensificar la cooperación estatal y llevar a cabo una política penal común en la prevención del cibercrimen, mediante una legislación apropiada y la mejora de la cooperación. Esta norma es el resultado de la preocupación por el uso de las redes y la información electrónica para la comisión de infracciones penales y la conciencia de que sus pruebas puedan ser almacenadas y transmitidas por estos medios. Por ello, según dispone el texto del Preámbulo se trata de salvaguardar "*la confidencialidad, la integridad y la disponibilidad de los sistemas informáticos, de las redes y de los datos*", pero de forma equilibrada entre la represión y el respeto de los derechos de los ciudadanos.

El Convenio comprende en su Capítulo II, entre las medidas que deben ser adoptadas en el ámbito nacional, las normas de Derecho penal material (Sección 1) y las normas de Derecho penal procesal (Sección 2). Las normas de derecho material abarcan: (i) los delitos contra la confidencialidad, integridad y disponibilidad de los datos y sistemas informáticos (Título 1); (ii) la falsedad y estafa informáticas (Título 2); (iii) las infracciones relativas a la pornografía infantil (Título 3); y (iv) las infracciones relativas a la propiedad intelectual y

---

*controversias. 1. Se mantendrá informado al Comité Europeo de Problemas Penales del Consejo de Europa (CDPC) acerca de la interpretación y aplicación del presente Convenio. 2. En caso de controversia entre las Partes sobre la interpretación o aplicación del presente Convenio, éstas intentarán resolver la controversia mediante negociaciones o por cualquier otro medio pacífico de su elección, incluida la sumisión de la controversia al CDPC, a un tribunal arbitral cuyas decisiones serán vinculantes para las Partes o a la Corte Internacional de Justicia, según acuerden las Partes interesadas*".

derechos conexos (Título 4). Además, está previsto que los Estados miembros adopten las medidas para sancionar la "*complicidad deliberada con vistas a la comisión de alguno de los delitos previstos en aplicación de los artículos 2 a 10*" (artículo 11.1) y adoptar las medidas necesarias para "*tipificar como delito en su derecho interno toda tentativa deliberada de cometer alguno de los delitos previstos en aplicación de los artículos 3 a 5, 7, 8, 9.1.a) y 9.1.c) del presente Convenio*" (artículo 11.2), si bien "*Las partes podrán reservarse el derecho a no aplicar, en todo o en parte, el párrafo 2 del presente artículo*" (artículo 11.3).

En nuestro caso, aunque el artículo 11.3 del Convenio no se refiere a las conductas de acceso al sistema informático, que se tipifican en su artículo 2, la regulación de la tentativa ya estaba prevista en el artículo 16 del CP. Por tanto, si como se expondrá en el Capítulo III se considera como bien jurídico protegido la seguridad de los sistemas de información, describiendo el tipo el acceso, tal y como veremos la consecuencia será su configuración como un delito de resultado, donde, como señala HURTADO ADRIÁN, será posible la tentativa, bien porque se inicia la acción pero el sujeto no es capaz de vulnerar las medidas de seguridad, dando lugar a la tentativa inacabada, o bien porque consiguiendo quebrantar esas medidas, no consigue el acceso al sistema (tentativa acabada)[145].

[145] En este sentido, HURTADO ADRIÁN, A., "Accesos informáticos ilícitos", en JUANES PECES, A. (Dir.) y VVAA, *Reforma del Código penal. Perspectiva económica tras la entrada en vigor de la Ley Orgánica 5/2010*

Por otra parte, también se establece que las Partes adopten las medidas necesarias para la sanción de las personas jurídicas cuando lleven a cabo algunas de las infracciones (artículo 12).

El acceso ilícito a los sistemas informáticos se encuentra regulado en su artículo 2[146]. La redacción del precepto nos lleva a cuestionar la pretendida armonización legislativa del Convenio por cuanto aunque ese intrusismo informático ilícito está previsto como infracción penal, se otorga libertad a los Estados miembros para que decidan si exigen o no vulneración de medidas de seguridad, la intención delictiva y que el sistema esté o no conectado a otro en la tipificación de estas conductas. Hubiera sido deseable una mayor rotundidad en una materia en la que se pretende armonizar las legislaciones nacionales y dar una respuesta coordinada y eficaz al fenómeno *hacking*, por lo que no se entiende el amplio marco de libertad dejado a los Estados firmantes, a los que sólo se les exige que regulen como infracción penal el acceso doloso no autorizado a todo o parte de un sistema informático.

---

*de 22 de junio. Situación jurídico-penal del empresario*, ed. El Derecho, Madrid, 2010, p. 130.

146 El artículo 2 del Convenio dispone que "*Las Partes adoptarán las medidas legislativas o de otro tipo que se estimen necesarias para prever como infracción penal, conforme a su derecho interno, el acceso doloso y sin autorización a todo o parte de un sistema informático. Las Partes podrán exigir que la infracción sea cometida con vulneración de medidas de seguridad, con la intención de obtener los datos informáticos o con otra intención delictiva, o también podrán requerir que la infracción se perpetre en un sistema informático conectado a otro sistema informático*".

#### *4.2.1.2 La DM 2005/222/JAI.*

Tal y como se ha indicado en el epígrafe 2, la DM 2005/222, relativa a los ataques de los que son objeto los sistemas de información, fue emitida por el Consejo de la Unión Europea en fecha 24 de febrero de 2005. Según se expone en sus considerandos, con esta norma se trata de reforzar la cooperación entre las autoridades de los Estados miembros de la Unión Europea aproximando las legislaciones penales en los ataques a los sistemas de información. La decisión se adopta porque se ha constatado la existencia de este fenómeno y la necesidad de actuar globalmente para poder responder eficazmente a esta amenaza, por cuanto los sistemas de información tienen una naturaleza transfronteriza que también suelen tener los ataques dirigidos contra ellos.

Por ello, conforme a esos considerandos, con la DM 2005/222 se establece la necesidad de legislar los delitos de acceso ilegal a sistemas de información y delitos de intromisión ilegal en sistema o en los datos, evitando una tipificación excesiva, atendido el hecho de que los citados objetivos pueden alcanzarse mejor en el ámbito de la Unión Europea que si se adoptaran las medidas legislativas individualmente por los Estados miembros, conforme a los principios de subsidiariedad y proporcionalidad. Así, según su Considerando 17, se trata de "*garantizar que los ataques contra los sistemas de información sean castigados en todos los Estados miembros mediante sanciones penales efectivas, proporcionadas y disuasorias y mejorar y*

*fomentar la cooperación judicial superando las posibles complicaciones*", objetivos que "*no pueden ser alcanzados de manera suficiente por los Estados miembros, ya que las normas tienen que ser comunes y compatibles, y, por consiguiente, pueden lograrse mejor a escala de la Unión, ésta puede adoptar medidas, de acuerdo con el principio de subsidiariedad consagrado en el artículo 5 del Tratado CE*".

Esta Decisión no tiene la extensión del Convenio Europeo sobre Cibercriminalidad, sino que impone[147] a los Estados miembros que castiguen penalmente el acceso intencionado no autorizado a un sistema de información (artículo 2)[148], la perturbación de sistemas

---

147 Respecto al valor vinculante de las Decisiones comunitarias, como sabemos, son actos jurídicos obligatorios en todos sus elementos (artículo 288 de la versión consolidada del Tratado de Funcionamiento de la Unión Europea, publicada en el DOUE nº C 326 de 26 de octubre de 2012, disponible en http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=celex%3A12012E%2FTXT, consultado el 9 de enero de 2017), de tal manera que, como resume el Consejo de Estado en su Informe sobre la Inserción del Derecho europeo en el ordenamiento español, de fecha 14 de febrero de 2008, p. 258-264 (disponible en http://www.consejo-estado.es/pdf/europa.pdf, consultado el 9 de enero de 2017), el incumplimiento de la Decisión conllevaría una responsabilidad estatal, que puede ser de dos tipos: (i) frente a la Comunidad Europea, con el Recurso de incumplimiento para exigir responsabilidades al Estado incumplidor y que contiene una fase precontenciosa donde la Comisión, "*tras identificar una infracción de las normas comunitarias por un Estado miembro, le envía una carta de emplazamiento describiendo los términos de la infracción imputada, de modo que dicho Estado tenga la posibilidad de presentar sus observaciones, antes de que la Comisión fije su postura mediante un dictamen motivado (artículo 226 del Tratado CE)*"; o (ii) frente a los particulares como responsabilidad patrimonial del Estado.

148 Según ordena el artículo 2, "*1. Cada Estado miembro adoptará las*

informáticos (artículo 3)[149] y los daños a los datos y sistemas informáticos (artículo 4)[150].

Por tanto, la Decisión vuelve a referirse al acceso ilícito a sistemas informáticos en su artículo 2, como ya se hiciera en el Convenio, reiterando la previsión de que el acceso ilícito al sistema informático sea infracción penal, al menos en los casos más graves, y la libertad de los Estados miembros en cuanto a la exigencia de vulneración de medidas de seguridad, si bien sin referirse a la intención del sujeto ni a la conexión del sistema con otro.

Al igual que con la redacción del Convenio, en la DM 2005/222/JAI de nuevo nos encontramos con el problema de que la

---

*medidas necesarias para que el acceso intencionado sin autorización al conjunto o a una parte de un sistema de información sea sancionable como infracción penal, al menos en los casos que no sean de menor gravedad.*

*2. Cada Estado miembro podrá decidir que las conductas mencionadas en el apartado 1 sean objeto de acciones judiciales únicamente cuando la infracción se cometa transgrediendo medidas de seguridad*".

[149] El artículo 3 establece "*Intromisión ilegal en los sistemas de información. 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, deteriorando, alterando, suprimiendo o haciendo inaccesibles datos informáticos, sea sancionable como infracción penal, al menos en los casos que no sean de menor gravedad*".

[150] Este precepto dispone: "*Intromisión ilegal en los datos. 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 graveda.*".

pretendida armonización legislativa entre sus miembros se ve truncada por una excesiva permisividad en las directrices para la tipificación de las conductas de *hacking*, por cuanto difícilmente podrán perseguirse estas conductas uniformemente en el ámbito internacional si cada Estado opta por exigir o no la vulneración de medidas de seguridad o decide castigar penalmente, o no, las conductas menos graves. El citado artículo 2 de la norma comunitaria sólo exige que se castigue como infracción penal por cada Estado miembro el "*acceso intencionado sin autorización al conjunto o una parte de un sistema de información … al menos en los casos que no sean de menor gravedad*", y aunque el anterior artículo 197.3 CP introducido por la LO 5/2010 ha cumplido con ese mínimo, cada legislador nacional ha podido decidir los elementos del tipo delictivo, lo que aleja esas legislaciones de la pretendida armonización y coordinación sobre una materia que, como se viene exponiendo, tiene un claro carácter transfronterizo.

### *4.2.2 La reforma del año 2015 y la Directiva 2013/40/UE.*

En el caso de la reforma del Código Penal introducida por la LO 1/2015, viene motivada "*para ofrecer respuesta a la delincuencia informática en el sentido de la normativa europea*", llevando a cabo "*la transposición de la Directiva 2013/40/UE, de 12 de agosto, relativa a los ataques contra los sistemas de información y la*

*interceptación de datos electrónicos cuando no se trata de una comunicación personal*" (apartado XIII de su Preámbulo y en su Disposición final sexta).

La citada Directiva 2013/40/UE[151] "*por la que se sustituye la DM 2005/222/JAI del Consejo*", viene precedida de una serie de comunicaciones[152], propuestas y dictámenes[153]: la Comunicación de la Comisión de 31 de mayo de 2006, «*Una estrategia para una sociedad de la información segura - Diálogo, asociación y potenciación*» (COM (2006) 251 final - no publicada en el Diario Oficial)[154], que estaba dirigida a "*revitalizar la estrategia política europea en materia*

---

151 En este caso, según el artículo 288 de la versión consolidada del Tratado de Funcionamiento de la Unión Europea, "*La directiva obligará al Estado miembro destinatario en cuanto al resultado que deba conseguirse, dejando, sin embargo, a las autoridades nacionales la elección de la forma y de los medios*".

152 Conforme al artículo 1 del Protocolo sobre el cometido de los Parlamentos nacionales en la UE, las comunicaciones son "*documentos de consulta de la Comisión*" "*transmitidos directamente por la Comisión a los Parlamentos nacionales cuando se publiquen. La Comisión transmitirá asimismo a los Parlamentos nacionales el programa legislativo anual, así como cualquier otro instrumento de programación legislativa o de estrategia política al mismo tiempo que los transmita al Parlamento Europeo y al Consejo*.". Protocolo publicado en el *DOUE, n° C 326 de 26 de octubre de 2012,* disponible en http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=celex%3A12012E%2FTXT, consultado el 10 de enero de 2017.

153 Según dispone el artículo 288 de la versión consolidada del Tratado de Funcionamiento de la Unión Europea, "*los dictámenes no serán vinculantes*".

154 Comunicación disponible en http://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=URISERV:l24153a&from=ES, consultado el 18 de septiembre de 2016.

*de seguridad de las redes y de la información*", trataba de "*definir los retos actuales y de proponer acciones para afrontarlos*" y optaba como estrategia por "*un enfoque multipartito que reúna a todas las partes interesadas. Este planteamiento se funda en el diálogo, la asociación y la responsabilización*", exponiendo entre sus "*retos principales*" que "*la seguridad sigue siendo un reto para todos: administraciones públicas, empresas y usuarios individuales. A menudo, los riesgos existentes se subestiman, siendo como es innegable la importancia del sector de las tecnologías de la información y las comunicaciones (TIC) para la economía y la sociedad europea. Además, otras infraestructuras críticas dependen cada vez más de la integridad de sus respectivos sistemas de información*"; la Comunicación de la Comisión de 12 de diciembre de 2006 sobre un "*Programa Europeo para la Protección de Infraestructuras Críticas*" [COM (2006) 786 final – Diario Oficial C 126 de 7 de junio de 2007][155], en el que "*se exponen los principios, procedimientos e instrumentos propuestos para aplicar el PEPIC*", siglas correspondientes al "*Programa Europeo para la Protección de Infraestructuras críticas*", que está dirigido a mejorar la protección de las infraestructuras críticas de la UE, estando previstas ayudas en este

[155] Comunicación en http://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=URISERV:l33260&from=ES, consultado el 18 de septiembre de 2016. Como infraestructuras críticas, define la Comunicación a las "*instalaciones, equipos físicos y de tecnología de la información, redes, servicios y activos cuya interrupción o destrucción pueden tener grandes repercusiones en la salud, la seguridad o el bienestar económico de los ciudadanos o en el funcionamiento de los gobiernos de los Estados miembros*.".

ámbito; la "*Comunicación de la Comisión al Parlamento Europeo, al Consejo y al Comité de las Regiones: Hacia una política general de lucha contra la ciberdelincuencia*" (COM (2007) 267 final de 22 de mayo de 2007)[156], donde se presenta "*una política general para coordinar mejor la lucha contra la ciberdelincuencia*"; 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 - «Proteger Europa de ciberataques e interrupciones a gran escala: aumentar la preparación, seguridad y resistencia»"* (COM/2009/0149 final)[157], que desarrolla la política europea de potenciar la seguridad de la sociedad de la información y la confianza en ella; la "*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*" (COM (2010) 517)[158], que tiene como objetivo sustituir la citada DM 2005/222/JAI; la "*Comunicación de la Comisión al Parlamento Europeo y al Consejo de 22 de noviembre de 2010 La Estrategia de Seguridad Interior de la UE en acción: cinco medidas para una Europa más segura*" (COM

156 *Vid*., *supra* nota 29.

157 Disponible en http://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:52009DC0149&qid=1441210483706&from=ES, consultado el 18 de septiembre de 2016.

158 Propuesta disponible en http://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:52010PC0517&qid=1441210865885&from=ES, consultado el 10 de enero de 2017.

(2010) 673 final no publicada en el Diario Oficial)[159], estableciendo como "*cinco objetivos estratégicos, con acciones específicas para cada objetivo*", los de "*desarticular las redes de la delincuencia internacional*", "*prevenir el terrorismo y abordar la radicalización y la captación*", "*aumentar los niveles de seguridad de los ciudadanos y las empresas en el ciberespacio*", "*reforzar la seguridad a través de la gestión de fronteras*" y "*reforzar la resistencia de Europa frente a la crisis y las catástrofes*"; y el "*Dictamen del Comité Económico y Social Europeo sobre la «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»*", de fecha 23 de julio de 2011, (COM(2010) 517 final — 2010/0273 (COD))[160], donde en líneas generales se acoge positivamente la Directiva propuesta, pidiendo que en el futuro se elabore un marco global para combatir la ciberdelincuencia y se insta a todos los Estados miembros a que la apoyen, también Reino Unido, Irlanda y Dinamarca, a pesar de las exenciones, para "*evitar que los delincuentes exploten las deficiencias de las políticas en el conjunto de la Unión*".

De nuevo se expone en los considerandos de la Directiva la necesidad de mejorar la cooperación entre las autoridades de los

[159] Comunicación disponible en http://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=URISERV:jl0050&from=ES, consultado el 10 de enero de 2017.

[160] Dictamen disponible en http://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:52011AE0816&from=ES, consultado el 10 de enero de 2017.

Estados miembros de la Unión Europea aproximando las legislaciones penales en los ataques a los sistemas de información tomando como marco el Convenio Europeo sobre Cibercriminalidad del año 2001. La Directiva se justifica por la importancia de los sistemas de información en la Unión para la interacción política, social y económica, siendo los ataques a estos sistemas una amenaza creciente en el ámbito comunitario.

En lo que se refiere a las conductas relacionadas con los ataques a los sistemas de información, la Directiva impone a los Estados miembros la obligación de adoptar las medidas necesarias conforme al "*Acceso ilegal a los sistemas de información*" previsto en su artículo 3, "*Interferencia ilegal en los sistemas de información*" (artículo 4), "*Interferencia ilegal en los datos*" (artículo 5) e "*Interceptación ilegal*" (artículo 6), quedando sustituida la Decisión marco 2005/222/JAI (artículo 15).

Por tanto, la Directiva vuelve a incluir el acceso ilícito y amplía las conductas anteriormente previstas en la DM 2005/222 con la incorporación de la interceptación ilegal[161].

[161] El artículo 6 de la Directiva establece "*Los Estados miembros adoptarán las medidas necesarias para garantizar que la interceptación, 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, intencionalmente y sin autorización, sea sancionable como infracción penal, al menos en los casos que no sean de menor gravedad*". Como interceptación de comunicaciones se entiende en el Diccionario del español jurídico "escucha o grabación del contenido de una comunicación,

En definitiva, en la medida que las nuevas tecnologías de la información y la comunicación dejan de ser novedosas para convertirse en medios cotidianos, se hace necesario cubrir las nuevas lagunas en el ordenamiento jurídico[162]. En este sentido, la Exposición de Motivos del Proyecto de la LO 5/2010 disponía en su publicación del BOCG de 15 de enero de 2007, núm. 119-1[163], que la tutela penal de la intimidad y los secretos viene exigiendo cada vez más medidas legales como consecuencia del incremento de los riesgos por el uso de las vías tecnológicas, que hacen posible la vulneración de la privacidad o los datos ubicados en sistemas informáticos. Por ello, existía una laguna normativa que exigía la reforma del artículo 197 del CP incorporando el acceso ilícito a datos o programas informáticos contenidos en sistemas informáticos, que además se lleva a cabo con la LO 5/2010 para cumplir con la DM 2005/222 y con la LO 1/2015 para la transposición de la Directiva 2013/40/UE, por la que se sustituye la Decisión marco 2005/222/JAI del Consejo dando como plazo de transposición hasta el 4 de septiembre de 2015 (artículo 16).

Precisamente, el que fuera el artículo 197.3 y actualmente es el nuevo artículo 197 *bis* 1 vienen referidos a los accesos ilícitos a los

---

o captación de sus datos, durante su transmisión" en MUÑOZ MACHADO, S. (Dir.) y VVAA, *Diccionario del español jurídico ...*, *cit*., nota 104, p. 958. En nuestro CP estas conductas se tipifican en los artículos 197, 278, 535 y 536.

[162] QUERALT JIMÉNEZ, J. J., *Derecho Penal Español. Parte Especial*, ed. Atelier, sexta edición, Barcelona, 2010, §8.

[163] Disponible en http://www.congreso.es/public_oficiales/L8/CONG/BOCG/A/A_119-01.PDF, consultado el 18 de septiembre de 2016.

sistemas informáticos y, aunque su inclusión en la reforma llevada a cabo por la LO 5/2010 fue inicialmente cuestionada en el Informe que emitió el CGPJ al Anteproyecto de 2006[164] tal y como se expone en el siguiente subepígrafe, la tipificación de estas conductas constituye una de las novedades introducidas por la LO 5/2010 por venir así establecido en la DM 2005/222, relativa a los ataques de los que son objeto los sistemas de información (artículos 2, 3 y 4), y en el Convenio del Consejo de Europa sobre Cibercriminalidad firmado en Budapest el 23 de noviembre de 2001 (artículo 2), siendo objeto de una nueva reforma por la LO 1/2015 en cumplimiento de la Directiva 2013/40/UE.

Son por tanto los motivos expuestos relativos a la necesidad de una normativa armonizada ante la peligrosidad de las nuevas

---

164 El texto del Informe del CGPJ al Anteproyecto de 2006 de Ley Orgánica por la que se modifica la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal, se encuentra disponible en http://www.juecesdemocracia.es/cgpj/2006/octubre/020de.06.pdf (consultado el 18 de septiembre de 2016). En concreto, la tipificación de estas nuevas conductas en el artículo 197.3 del CP se cuestionaba en los siguientes términos: "*lo cierto es que el atentado contra la privacidad de los sistemas de información se encuentra formalmente sancionado, incluso con penas más severas, en el apartado 2 del propio artículo 197 CP, cuyo inciso final prevé la imposición conjunta de las penas de prisión de uno a cuatro años y multa de doce a veinticuatro meses al que, sin estar autorizado, acceda por cualquier medio a ficheros o soportes informáticos, electrónicos o telemáticos, sin exigir siquiera que para ello se vulneren o neutralicen las medidas de seguridad dispuestas para impedir tal tipo de injerencias.*". De esta forma se apuntaba hacia una supuesta reiteración de tipos. Sin embargo, tal y como veremos, las diferencias entre el artículo 197.2 y el nuevo tipo del artículo 197.3 del CP son numerosas, empezando por el bien jurídico protegido.

tecnologías los que fundamentan la regulación internacional y con ella la introducción de estas conductas en nuestro Código Penal de 1995 con la reforma del artículo 197.3 en fecha 22 de junio de 2010 y su modificación en fecha 30 de marzo de 2015 incorporando el artículo 197 *bis*.

Por último, conviene destacar que las citadas reformas no han estado exentas de críticas en lo que se refiere a la regulación de los delitos contra la intimidad comprendidos en el artículo 197 CP, especialmente por su ubicación sistemática, por cuanto, tal y como se expondrá en el Capítulo III, no estamos ante un delito que afecte directamente a la intimidad. En este sentido, entre otros, TOMÁS-VALIENTE LANUZA[165], critica que la ubicación sistemática de este delito en función de su bien jurídico protegido conlleva dificultades en la interpretación del precepto.

Por su parte, ANARTE BORRALLO y DOVAL PAÍS[166], han destacado que con la reforma del artículo 197.3 CP del año 2010 se evidencia la "*imparable –pero inútil y contraproducente- escalada del Derecho penal hacia el "riesgo cero".* MORALES PRATS[167] ha

---

165 TOMÁS-VALIENTE LANUZA, C., "Título X. Delitos contra la Intimidad ...", *cit*., nota 127, p. 802.

166 ANARTE BORRALLO, E. y DOVAL PAIS, A., "Delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio (1). Delitos contra la intimidad y los datos personales", en BOIX REIG, J. (Dir.) y VVAA. *Derecho Penal. Parte Especial. Volumen I. La protección penal de los intereses jurídicos personales (adaptado a las reformas de 2010 del Código penal),* ed. Iustel, primera edición, Madrid, 2010, p. 455.

167 MORALES PRATS, F., "La reforma de los delitos contra la intimidad

resaltado la creación de tipos penales con una intervención excesiva, contraviniendo la claridad sistemática inicialmente planteada en los tipos del Código Penal de 1995, la incriminación de actos preparatorios con los problemas que planteará su delimitación en la esfera del desvalor, la oportunidad desaprovechada para mejorar técnicamente el acceso ilícito informático a la intimidad, el empeoramiento de los tipos agravados, concluyendo con una "*valoración desoladora*", pareciendo que "*las reformas penales respondieran a una máquina infernal, desbocada y fuera del alcance del control humano, encaminada a reformas sin fin del Código Penal en claro desprecio a los patrones del Estado de Derecho, y a los valores que incorpora, en especial, la seguridad jurídica*", mientras que otros autores como COLÁS TURÉGANO[168] han mencionado la posibilidad de que con la reforma de 2015 se hubiese creado un título específico dedicado a los delitos contra la seguridad de los sistemas informáticos.

Finalmente, no han faltado autores que se han referido a la reforma de 2015 como "*una jungla de preceptos nuevos de los que no es posible apreciar, en una primera aproximación, cuál es el alcance de la reforma y cuáles son sus novedades frente a la legislación penal*

---

artículo 197 CP", en QUINTERO OLIVARES, G. (Dir.), y VVAA, *Comentario a la reforma penal de 2015*, ed. Aranzadi, Navarra, 2015, p. 459 y 460.

[168] COLÁS TURÉGANO, A., "Nuevas conductas delictivas contra la intimidad (arts. 197, 197 bis, 197 ter)", en GONZÁLEZ CUSSAC, J. L. (Dir.) y VVAA, *Comentarios a la reforma del Código penal de 2015*, ed. Tirant lo Blanch, Valencia, 2015, p.663.

*que se deroga*"[169] o, en general, al hecho de que "*la Sección Penal de la Comisión General de Codificación no interviniera nunca en el largo proceso que culminó con el Código Penal de 1995 y que tampoco haya sido convocada en relación con sus numerosas reformas*" y que "*Quizá esta ausencia explique la precipitación de algunos de los cambios. Al parecer, siempre se ha preferido recurrir a grupos de expertos escogidos <<ad hoc>> por el Ministro de Justicia*"[170].

En definitiva, parece que las últimas reformas comentadas ponen de manifiesto la falta de un criterio sistemático claro por parte del legislador nacional y comunitario, así como el caos que encuentra el intérprete en el momento de intentar llevar a cabo un análisis organizado que pueda justificar las continuas modificaciones normativas. Frente a esa sucesión interminable de normas comunitarias, basadas en el continuo cambio sobre la materia, se podría haber aportado cierto orden y claridad con la elaboración de una única norma comunitaria, clara, precisa y congruente, con vistas a su permanencia en el tiempo, que hubiese regulado las conductas básicas de *hacking* y dejase para el desarrollo futuro tan solo las cuestiones técnicas y accesorias ligadas a la acelerada evolución de las nuevas tecnologías.

---

169 GIMBERNAT ORDEIG, E., "Prólogo", en MANZANARES SAMANIEGO, J. L., *La reforma del Código penal de 2015 conforme a las Leyes Orgánicas 1 y 2/2015, de 30 de marzo*, ed. La Ley, Madrid, 2015, p. 17.

170 MANZANARES SAMANIEGO, J.L., *La reforma del Código penal de 2015 conforme a las Leyes Orgánicas 1 y 2/2015, de 30 de marzo*, ed. La Ley, Madrid, 2015, p.26.

### *4.3 La tramitación parlamentaria de las reformas de los años 2010 y 2015.*

#### *4.3.1 La reforma del año 2010.*

La modificación llevada a cabo en el Código Penal por la LO 5/2010, con la que por primera vez se introducen las conductas de *hacking*, ha tenido una dilatada tramitación parlamentaria desde que en fecha 14 de julio de 2006 el Consejo de Ministros hiciera referencia a la recepción del Informe del Ministro de Justicia sobre el Anteproyecto de Ley Orgánica por la que se modifica la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal[171]. El Consejo consideraba que el texto era la respuesta a las nuevas modalidades delictivas y a la necesaria armonización con la legislación europea. Entre esas nuevas formas de delincuencia, el Gobierno mencionaba los delitos basados en las nuevas tecnologías, incluyendo las intromisiones ilegales en los sistemas informáticos ajenos.

Desde entonces se ha venido reiterando esa necesidad de modernizar el Código Penal de 1995, tanto en la Exposición de Motivos del Proyecto de Ley Orgánica por la que se modifica el Código Penal, publicada en el BOCG de 15 de enero de 2007, núm.

[171] La referencia al Informe se encuentra disponible en http://www.lamoncloa.gob.es/consejodeministros/referencias/Paginas/2006/refc20060714.aspx#C%C3%B3digoPenal, consultado el 18 de septiembre de 2016.

119-1[172], en el texto del Anteproyecto finalmente aprobado por el Consejo de Ministros el 23 de julio de 2009[173], como en la redacción

[172] Disponible en http://www.congreso.es/public_oficiales/L8/CONG/BOCG/A/A_119-01.PDF, consultado el 18 de septiembre de 2016. En relación con el que sería finalmente el artículo 197.3, el texto de este Proyecto todavía no incluía las conductas de mantenimiento no autorizado en el sistema informático ni la responsabilidad de las personas jurídicas, limitando el precepto al siguiente contenido: "*En el artículo 197 se introduce un nuevo apartado 3, pasando los actuales apartados 3, 4, 5 y 6 a ser los apartados 4, 5, 6 y 7, y se añade el apartado 8, que quedan redactados como siguen: «3. El que por cualquier medio o procedimiento y vulnerando las medidas de seguridad establecidas para impedirlo, accediera sin autorización a datos o programas informáticos contenidos en un sistema informático o en parte del mismo, será castigado con pena de prisión de seis meses a dos años.»*

*«8. Si los hechos descritos en los apartados anteriores se cometiesen en el seno de una organización criminal, se aplicarán respectivamente las penas superiores en grado.»".*

[173] Texto del Anteproyecto disponible en http://www.juecesdemocracia.es/LegislacionActual/CP_Antepro_23_07_09.pdf, consultado el 18 de septiembre de 2016. El texto del Anteproyecto finalmente aprobado por el Consejo de Ministros el 23 de julio de 2009 introduce como novedad respecto al texto anterior la referencia al mantenimiento no autorizado en un sistema informático y la responsabilidad de las personas jurídicas por estos delitos: "*En el artículo 197 se introduce un nuevo apartado 3, pasando los actuales apartados 3, 4, 5 y 6 a ser los apartados 4, 5, 6 y 7, y se añade el apartado 8, que quedan redactados como siguen: «3. El que por cualquier medio o procedimiento y vulnerando las medidas de seguridad establecidas para impedirlo, accediera 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.*

*Cuando del delito fuere responsable una persona jurídica de acuerdo con lo establecido en el artículo 31 bis de este Código, se le impondrá la pena de multa del tanto al duplo del perjuicio causado.*

*8. Si los hechos descritos en los apartados anteriores se cometiesen en el*

del Proyecto publicada en el BOCG de 27 de noviembre de 2009, núm. 52-1, a la que nos referimos a continuación[174], o en la definitiva LO 5/2010.

Esa armonización y respuesta a los nuevos comportamientos delictivos fue también manifestada en las numerosas enmiendas propuestas al Proyecto, a las que se hace referencia en las siguientes páginas, desde la citada publicación en el BOCG de 27 de noviembre de 2009 hasta la aprobación de la LO 5/2010[175]. En cuanto afecta al artículo 197, tanto en la Exposición de Motivos del Anteproyecto aprobado el 23 de julio de 2009 como en el texto publicado el 27 de

---

*seno de una organización o grupo criminales, se aplicarán respectivamente las penas superiores en grado.»".*

[174] El texto del Proyecto publicado en el BOCG en fecha 27 de noviembre de 2009 está disponible en http://www.congreso.es/public_oficiales/L9/CONG/BOCG/A/A_052-01.PDF#page=1, consultado el 18 de septiembre de 2016. Este texto ya incluye el segundo grupo de conductas relativas al mantenimiento no autorizado en sistemas informáticos: "*3. 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.*".

[175] Las enmiendas y diarios de sesiones, a las que se hace referencia en las siguientes páginas en relación con el Proyecto de la que finalmente sería la LO 5/2010, se encuentran disponibles en http://www.congreso.es/portal/page/portal/Congreso/Congreso/Iniciativas?_piref73_2148295_73_1335437_1335437.next_page=/wc/servidorCGI&CMD=VERLST&BASE=IWI9&FMT=INITXDSS.fmt&DOCS=1-1&DOCORDER=FIFO&OPDEF=ADJ&QUERY=%28121%2F000052*.NDOC.%29, consultado el 18 de septiembre de 2016.

noviembre de 2009 se aludía a las directrices de la DM 2005/222 para explicar la ubicación de estas conductas en dos artículos distintos, uno relativo a los daños y el otro junto al descubrimiento y revelación de secretos, donde se encontraría el acceso y el mantenimiento no autorizado en sistemas informáticos.

En este sentido, el segundo grupo de conductas relativo al mantenimiento no autorizado en sistemas informáticos no aparecía en el texto del Anteproyecto aprobado por el Consejo de Ministros el 14 de noviembre de 2008, ni en los textos internacionales de los que traía causa la reforma, constituyendo una de las novedades introducidas en el Anteproyecto aprobado el 23 de julio de 2009 y en el Proyecto publicado el 27 de noviembre de 2009.

Siguiendo el texto del Anteproyecto, el Proyecto establecía en un nuevo apartado 3 del artículo 197 la conducta de *hacking* e introducía en su apartado 8 la previsión del delito cometido por organización o grupo criminal en los siguientes términos[176]: "*En el*

[176] El artículo 31 *bis*, al que se remitía el artículo 197.3, quedaba redactado así: *"1. En los supuestos previstos en este Código, las personas jurídicas serán penalmente responsables de los delitos cometidos, en nombre o por cuenta de las mismas, y en su provecho, por sus representantes legales, los administradores de hecho o de derecho o los empleados con facultades de obligar a dicha persona jurídica.*
*En los mismos supuestos, las personas jurídicas serán también penalmente responsables de los delitos cometidos, en el ejercicio de actividades sociales y por cuenta y en provecho de las mismas, por quienes, estando sometidos a la autoridad de las personas físicas mencionadas en el párrafo anterior, han podido realizar los hechos por no haberse ejercido sobre ellos el debido control.*

*2. La responsabilidad penal de las personas jurídicas no excluirá la*

*de las personas físicas a que se refiere el apartado anterior, ni la de éstas excluirá la responsabilidad penal de aquéllas. Cuando como consecuencia de los mismos hechos se impusiere a ambas la pena de multa, los Jueces o tribunales modularán las respectivas cuantías de modo que la suma resultante no sea desproporcionada en relación con la gravedad de aquéllos.*

*3. La concurrencia, en las personas que materialmente hayan realizado los hechos o en las que los hubiesen hecho posibles por no haber ejercido el debido control, de circunstancias que afecten la culpabilidad del acusado o agraven su responsabilidad, o el hecho de que dichas personas hayan fallecido o se hubieren sustraído a la acción de la justicia, no excluirá ni modificará la responsabilidad penal de las personas jurídicas, sin perjuicio de lo que se dispone en el apartado siguiente.*

*4. Serán circunstancias atenuantes de la responsabilidad penal de las personas jurídicas haber realizado, con posterioridad a la comisión del delito y a través de sus representantes legales, las siguientes actividades: a) Haber procedido antes de conocer que el procedimiento judicial se dirige contra ella, a confesar la infracción a las autoridades. b) Haber colaborado en la investigación del hecho aportando pruebas, en cualquier momento del proceso, que fueran nuevas y decisivas para declarar su responsabilidad. c) Haber procedido en cualquier momento del procedimiento y con anterioridad al juicio oral a reparar o disminuir el daño causado por el delito. d) Haber establecido, antes del comienzo del juicio oral, medidas eficaces para prevenir y descubrir los delitos que en el futuro pudieran cometerse con los medios o bajo la cobertura de la persona jurídica.*

*5. Las disposiciones relativas a la responsabilidad penal de las personas jurídicas no serán aplicables al Estado, a las Administraciones Públicas territoriales e institucionales, a los Organismos Reguladores, las Agencias y Entidades Públicas Empresariales, a los partidos políticos y sindicatos, a las organizaciones internacionales de derecho público, ni a aquellas otras que ejerzan potestades públicas de soberanía, administrativas o cuando se trate de Sociedades mercantiles Estatales que ejecuten políticas públicas o presten servicios de interés económico general.*

*En estos supuestos, los órganos jurisdiccionales podrán efectuar declaración de responsabilidad penal en el caso de que aprecien que se trata de una forma jurídica creada por sus promotores, fundadores, administradores o representantes con el propósito de eludir una eventual responsabilidad penal".*

*artículo 197 se introduce un nuevo apartado 3, pasando los actuales apartados 3, 4, 5 y 6 a ser los apartados 4, 5, 6 y 7 y se añade el apartado 8, que quedan redactados como siguen:* "*3. 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.*

*Cuando del delito fuere responsable una persona jurídica de acuerdo con lo establecido en el artículo 31 bis de este Código, se le impondrá la pena de multa del tanto al duplo del perjuicio causado.*

*8. Si los hechos descritos en los apartados anteriores se cometiesen en el seno de una organización o grupo criminales, se aplicarán respectivamente las penas superiores en grado*".

El encargo del dictamen sobre el Proyecto a la Comisión de Justicia y la orden de la publicación del Proyecto en el BOCG, estableciendo quince días para enmiendas, fue llevado a cabo en fecha 24 de noviembre de 2009 por la Mesa del Congreso, plazo que una vez publicado concluía el 16 de diciembre de 2009. Sin embargo, este período fue sucesivamente ampliado por los acuerdos de la Cámara de 15 de diciembre de 2009, 21 de diciembre de 2009, 2 de febrero de 2010, 9 de febrero de 2010, 16 de febrero de 2010, 23 de febrero de 2010 y 2 de marzo de 2010. En fecha 11 de marzo de 2010 se publicaba en el Diario de Sesiones del Congreso de los Diputados el

debate de totalidad del Proyecto, por el que el Ministro de Justicia, Sr. Caamaño Domínguez, defendía la reforma en cuanto a la responsabilidad penal de las personas jurídicas, acorde con otros ordenamientos jurídicos y para evitar la denominada irresponsabilidad organizada, así como la necesaria incorporación de la normativa europea en materias tales como los delitos informáticos.

En defensa de las enmiendas a la totalidad, el Grupo Parlamentario Mixto criticaba la orientación de la reforma hacia el endurecimiento de las penas, por cuanto consideraban que se buscaba la solución a cualquier conflicto con el Código Penal. Por su parte, el Grupo Parlamentario Vasco (EAJ-PNV) también resaltaba la instrumentalización del Código Penal ante los acontecimientos sociales.

El Grupo Parlamentario de Esquerra Republicana-Izquierda Unida-Iniciativa per Catalunya Verds exponía sus enmiendas manifestando su rechazo a que las reformas penales se realizasen atendiendo a los medios de comunicación.

En cuanto al Grupo Catalán (Convergència i Unió), defendía sus enmiendas para comenzar una negociación, entendiendo que era necesaria la reforma del Código Penal y debatir sobre esa reforma.

Por último, el Grupo Parlamentario Popular pretendía la tramitación de la reforma, al igual que el Grupo Parlamentario Socialista.

Las propuestas fueron finalmente publicadas en el BOCG de 18 de marzo de 2010, nº 52-9. Entre las que afectan a las conductas que nos ocupan, diversos grupos políticos presentaron enmiendas a la totalidad, que si bien por lo general no discutían la necesidad de armonizar la normativa cuando lo imponen las obligaciones internacionales, sí criticaban la utilización del Código Penal para resolver cualquier conflicto. En este sentido se manifestaban el BNG con la enmienda nº 2, el Grupo Parlamentario Vasco (EAJ-PNV), con la enmienda nº 3, y el Grupo Parlamentario de Esquerra Republicana-Izquierda Unida-Iniciativa per Catalunya-Verds, presentando la enmienda nº 4.

En cuanto a la modificación específica del artículo 197 del CP, la enmienda nº 29, presentada por el Grupo Parlamentario de Esquerra Republicana-Izquieda Unida-Iniciativa per Catalunya-Verds, proponía la supresión de su apartado 8, relativo a la comisión de estos delitos en el seno de una organización o grupos criminales, por cuanto entendían que la referencia a grupo suponía incluir acuerdos ocasionales para delinquir, lo cual caracteriza toda codelincuencia y supone generalizar el endurecimiento de la pena.

También se propuso la modificación sobre el artículo 31 *bis*, relativo a la responsabilidad penal de las personas jurídicas, al que se remitía finalmente el artículo 197.3 del CP. En concreto, el Grupo Parlamentario Vasco (EAJ-PNV) propuso la supresión del artículo 31 *bis* con la enmienda nº 99, ya que sería necesario determinar las personas a los que se van a atribuir las conductas posteriores al delito

en cuanto a la atenuación de la responsabilidad penal de la persona jurídica, además sería preciso reformar la Ley de Enjuiciamiento Criminal en materia de imputación y la regulación de las relaciones jurídico procesales con las personas jurídicas.

Por su parte, el Grupo Parlamentario Catalán (Convergència i Unió) defendía con la enmienda nº 141 la supresión de todas las disposiciones relativas a la responsabilidad penal de las personas jurídicas, para que fuese llevado a una Ley penal independiente, de esta forma se evitaba una interpretación sistemática en el Código Penal que podría conducir a una revisión de la acción y culpabilidad hacia una tendencia objetiva, llevando a recibir de otras ramas del ordenamiento la denominada responsabilidad objetiva.

Este mismo grupo parlamentario propuso dos enmiendas del artículo 31 *bis*. La primera, la nº 145, pretendía añadir una nueva redacción al apartado 1[177] justificada en la necesidad de ceñir la responsabilidad social de las personas jurídicas a las conductas llevadas a cabo en el ámbito de sus actividades sociales, y la segunda, la nº 146, se refería al segundo párrafo[178] del artículo 31 *bis*,

---

177 El nuevo texto presentado dispondría *"1. En los supuestos previstos en este Código, las personas jurídicas serán penalmente responsables de los delitos cometidos en el ejercicio de sus actividades sociales, en nombre o por cuenta de las mismas, y en su provecho, por sus representantes legales o los administradores de hecho o de derecho.".*

178 La enmienda proponía la siguiente redacción: *"En los mismos supuestos, las personas jurídicas serán también penalmente responsables de los delitos cometidos, en el ejercicio de actividades sociales y por cuenta y en provecho de las mismas, por quienes, estando sometidos a la autoridad*

basándola en la imprecisión que suponía la simple referencia al "*debido control*", proponiendo que fuera en el ejercicio de actividades sociales y además que la falta de control fuera debida a imprudencia grave.

El Grupo Parlamentario Popular en el Congreso presentó la enmienda nº 335, cambiando la redacción del artículo 31 *bis*, apartado 2[179], por entender que el principio de legalidad exige una mejora técnica conforme a la cual se determine en este apartado la pena a imponer, a diferencia de la previsión del Proyecto, donde se dejaba en manos de los órganos jurisdiccionales decidir la pena de multa a imponer. Por los mismos motivos de mejora de redacción, este grupo también propuso la modificación del artículo 31 *bis*, apartado 4[180], en cuanto consideraban que debía precisarse si las atenuantes previstas en este apartado eran aplicables a las personas jurídicas o también eran

---

*de las personas físicas mencionadas en el párrafo anterior, han podido realizar los hechos por no haberse ejercido sobre ellos el debido control, siempre que dicha falta de control se haya debido a imprudencia grave de dichas personas físicas.".*

[179] La redacción propuesta era la siguiente: *"2. La responsabilidad penal de las personas jurídicas no excluirá la de las personas físicas a que se refiere el apartado anterior, ni la de éstas excluirá la responsabilidad penal de aquéllas. Cuando como consecuencia de los mismos hechos se impusiere a ambas la pena de multa, los juzgados o tribunales impondrán la multa del tanto al séxtuplo de modo que la suma resultante no sea desproporcionada en relación con la gravedad de aquéllos.".*

[180] El nuevo apartado 4 propuesto comenzaría: "*Respecto de la responsabilidad penal de las personas jurídicas sólo podrán considerarse como circunstancias atenuantes haber realizado, con posterioridad a la comisión del delito y a través de sus representantes legales, las siguientes actividades:*".

aplicables a las personas físicas. Por otra parte, su enmienda nº 337 tenía por objeto la modificación del apartado 5[181], en la que consideraban conveniente excluir de la aplicación del precepto a las personas jurídicas que suponen un poder público, pero no a los partidos políticos ni a los sindicatos, por cuanto tenían su propia normativa especial y expresas previsiones en el Código Penal, ni tampoco la exclusión genérica de otras personas jurídicas que presten servicios esenciales a la comunidad.

Por último, en relación con el artículo 31 *bis*, el Grupo Parlamentario de Esquerra Republicana-Izquierda Unida-Iniciativa per Catalunya Verds propuso su supresión con la enmienda nº 236, en la medida en que consideraban una innecesaria doble regulación la existencia del régimen previsto en el artículo 129 del Código Penal e introducir el nuevo precepto dedicado a la responsabilidad penal de las personas jurídicas, cuando estas situaciones ya podían ser resueltas aplicando el citado artículo 129.

---

[181] El Grupo Parlamentario Popular en el Congreso proponía la siguiente redacción del artículo 31 *bis,* apartado 5: *"5. Las disposiciones relativas a la responsabilidad penal de las personas jurídicas no serán aplicables al Estado, a las Administraciones Públicas territoriales e institucionales, a los Organismos Reguladores, las Agencias y Entidades Públicas Empresariales, a las organizaciones internacionales de derecho público, ni a aquellas otras que ejerzan potestades públicas de soberanía.*
*En estos supuestos, los órganos jurisdiccionales podrán efectuar declaración de responsabilidad penal en el caso de que aprecien que se trata de una forma jurídica creada por sus promotores, fundadores, administradores o representantes con el propósito de eludir una eventual responsabilidad penal.".*

En fecha 21 de abril de 2010 se publicaba en el BOCG el Informe de la Ponencia dirigido a la Comisión de Justicia, proponiendo el rechazo de las enmiendas a la generalidad del Proyecto presentadas, la aceptación de una transacción respecto a las enmiendas presentadas al artículo 31 *bis* y el rechazo de la enmienda nº 29 presentada por el Grupo Parlamentario Esquerra Republicana-Izquierda Unida-Iniciativa per Catalunya Verds (ERC-IV-ICV), relativa al artículo 197[182], recomendando en este caso una transacción

[182] El texto del Proyecto acompañado al Informe establece en negrita las modificaciones que se proponen a los artículos 197.3 y 31 *bis,* al que se remite el 197.3, incluyendo un nuevo artículo 66 *bis* relativo a la aplicación de las penas a las personas jurídicas. En cuanto al artículo 197.3, "(…) *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 impondrá la pena de multa* ***de seis meses a dos años. 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****.".*

Y respecto al artículo 31 *bis* al que se remite el citado artículo 197.3, *"Se añade el artículo 31 bis, que tendrá la siguiente redacción:* ***1. En los supuestos previstos en este Código, las personas jurídicas serán penalmente responsables de los delitos cometidos en nombre o por cuenta de las mismas, y en su provecho, por sus representantes legales y administradores de hecho o de derecho.***

*En los mismos supuestos, las personas jurídicas serán también penalmente responsables de los delitos cometidos, en el ejercicio de actividades sociales y por cuenta y en provecho de las mismas, por quienes, estando sometidos a la autoridad de las personas físicas mencionadas en el párrafo anterior, han podido realizar los hechos por no haberse ejercido sobre ellos el debido control* ***atendidas las concretas circunstancias del caso.***

*2.* ***La responsabilidad penal de las personas jurídicas será exigible siempre que se constate la comisión de un delito que haya tenido que cometerse por quien ostente los cargos o funciones aludidas en el***

en relación con el nuevo artículo 66 *bis*, que se introducía en relación a las reglas de aplicación de las penas a las personas jurídicas. En concreto, conforme al artículo 66 *bis* propuesto, se establecía la obligación de estar a "*lo dispuesto en las reglas 1a a 4a y 6a a 8a del primer número del artículo 66*" y "*para decidir sobre la imposición y la extensión de las penas previstas en las letras b) a g) del apartado 7 del artículo 33 habrá de tenerse en cuenta: a) Su necesidad para*

---

***apartado anterior, aun cuando la concreta persona física responsable no haya sido individualizada o no haya sido posible dirigir el procedimiento contra ella****. Cuando como consecuencia de los mismos hechos se impusiere a ambas la pena de multa los* ***J****ueces o Tribunales modularán las respectivas cuantías, de modo que la suma resultante no sea desproporcionada en relación con la gravedad de aquéllos.*

*3. La concurrencia, en las personas que materialmente hayan realizado los hechos o en las que los hubiesen hecho posibles por no haber ejercido el debido control, de circunstancias que afecten* ***a*** *la culpabilidad del acusado o agraven su responsabilidad, o el hecho de que dichas personas hayan fallecido o se hubieren sustraído a la acción de la justicia, no excluirá ni modificará la responsabilidad penal de las personas jurídicas, sin perjuicio de lo que se dispone en el apartado siguiente.*

*4.* ***Sólo podrán considerarse*** *circunstancias atenuantes de la responsabilidad penal de las personas jurídicas haber realizado, con posterioridad a la comisión del delito y a través de sus representantes legales, las siguientes actividades: a) Haber procedido, antes de conocer que el procedimiento judicial se dirige contra ella, a confesar la infracción a las autoridades. b) Haber colaborado en la investigación del hecho aportando pruebas, en cualquier momento del proceso, que fueran nuevas y decisivas para* ***esclarecer las responsabilidades penales dimanantes de los hechos****. c) Haber procedido en cualquier momento del procedimiento y con anterioridad al juicio oral a reparar o disminuir el daño causado por el delito. d) Haber establecido, antes del comienzo del juicio oral, medidas eficaces para prevenir y descubrir los delitos que en el futuro pudieran cometerse con los medios o bajo la cobertura de la persona jurídica. 5.* (…).".

*prevenir la continuidad de la actividad delictiva o de sus efectos. b) Sus consecuencias económicas y sociales, y especialmente los efectos para los trabajadores. c) El puesto que en la estructura de la persona jurídica ocupa la persona física u órgano que incumplió el deber de control", "Cuando las penas previstas en las letras c) a g) del apartado 7 del artículo 33 se impongan con una duración limitada, ésta no podrá exceder la duración máxima de la pena privativa de libertad prevista para el caso de que el delito fuera cometido por persona física", "Para la imposición de las sanciones previstas en las letras c) a g) por un plazo superior a dos años será necesario que se dé alguna de las dos circunstancias siguientes: a) Que la persona jurídica sea reincidente. b) Que la persona jurídica se utilice instrumentalmente para la comisión de ilícitos penales. Se entenderá que se está ante este último supuesto siempre que la actividad legal de la persona jurídica sea menos relevante que su actividad ilegal"* y por último, *"Para la imposición con carácter permanente de las sanciones previstas en las letras b) y e), y para la imposición por un plazo superior a cinco años de las previstas en las letras e) y f) del apartado 7 del artículo 33, será necesario que se dé alguna de las dos circunstancias siguientes: a) Que se esté ante el supuesto de hecho previsto en la regla 5a del primer número del artículo 66. b) Que la persona jurídica se utilice instrumentalmente para la comisión de ilícitos penales. Se entenderá que se está ante este último supuesto siempre que la actividad legal de la persona jurídica sea menos relevante que su actividad ilegal".*

Como consecuencia de este Informe, en fecha 28 de abril de 2010 se introducía en el BOCG el Dictamen emitido por la Comisión de Justicia[183], por el que se modificaban entre otros el artículo 31 *bis*,

[183] El texto del artículo 66 *bis* no se modifica en el Dictamen, a diferencia de los citados artículos 31 *bis* y 197, donde en negrita se resalta la modificación que se transcribe a continuación: "*Se añade el artículo 31 bis, que tendrá la siguiente redacción: "**1. En los supuestos previstos en este Código, las personas jurídicas serán penalmente responsables de los delitos cometidos en nombre o por cuenta de las mismas, y en su provecho, por sus representantes legales y administradores de hecho o de derecho.***

*En los mismos supuestos, las personas jurídicas serán también penalmente responsables de los delitos cometidos, en el ejercicio de actividades sociales y por cuenta y en provecho de las mismas, por quienes, estando sometidos a la autoridad de las personas físicas mencionadas en el párrafo anterior, han podido realizar los hechos por no haberse ejercido sobre ellos el debido control **atendidas las concretas circunstancias del caso.***

*2. **La responsabilidad penal de las personas jurídicas será exigible siempre que se constate la comisión de un delito que haya tenido que cometerse por quien ostente los cargos o funciones aludidas en el apartado anterior, aun cuando la concreta persona física responsable no haya sido individualizada o no haya sido posible dirigir el procedimiento contra ella**. Cuando como consecuencia de los mismos hechos se impusiere a ambas la pena de multa**,** los **j**ueces o tribunales modularán las respectivas cuantías, de modo que la suma resultante no sea desproporcionada en relación con la gravedad de aquéllos.*

*3. La concurrencia, en las personas que materialmente hayan realizado los hechos o en las que los hubiesen hecho posibles por no haber ejercido el debido control, de circunstancias que afecten **a** la culpabilidad del acusado o agraven su responsabilidad, o el hecho de que dichas personas hayan fallecido o se hubieren sustraído a la acción de la justicia, no excluirá ni modificará la responsabilidad penal de las personas jurídicas, sin perjuicio de lo que se dispone en el apartado siguiente.*

*4. **Sólo podrán considerarse** circunstancias atenuantes de la responsabilidad penal de las personas jurídicas haber realizado, con posterioridad a la comisión del delito y a través de sus representantes*

se introducía el nuevo artículo 66 *bis* propuesto en el Informe, se proponía un nuevo artículo 197, y también se publicaban los escritos manteniendo las enmiendas para su debate en el Pleno.

Los textos de los artículos 31 *bis* y 197.3, modificados en el citado Dictamen, y del mencionado artículo 66 *bis*, fueron aprobados por el Pleno del Congreso de los Diputados y publicados en el BOCG de 6 de mayo de 2010, siendo remitidos en esta misma fecha por el Senado a la Comisión de Justicia y estableciéndose el 19 de mayo de 2010 como fecha límite para la presentación de enmiendas, fecha que sería ampliada hasta el 25 de mayo de 2010.

---

*legales, las siguientes actividades: a) Haber procedido, antes de conocer que el procedimiento judicial se dirige contra ella, a confesar la infracción a las autoridades. b) Haber colaborado en la investigación del hecho aportando pruebas, en cualquier momento del proceso, que fueran nuevas y decisivas para* ***esclarecer las responsabilidades penales dimanantes de los hechos****. c) Haber procedido en cualquier momento del procedimiento y con anterioridad al juicio oral a reparar o disminuir el daño causado por el delito. d) Haber establecido, antes del comienzo del juicio oral, medidas eficaces para prevenir y descubrir los delitos que en el futuro pudieran cometerse con los medios o bajo la cobertura de la persona jurídica. 5.* (…)*.".*

En cuanto al artículo 197, el texto del Dictamen establece en negrita las modificaciones propuestas y que a continuación se transcriben: *"En el artículo 197 se introduce un nuevo apartado 3, pasando los actuales apartados 3, 4, 5 y 6 a ser los apartados 4, 5, 6 y 7, y se añade* ***un*** *apartado 8,* ***con la siguiente redacción:*** *"3.* (…) *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 impondrá la pena de multa* ***de seis meses a dos años. 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****.".*

Las enmiendas a los artículos 31 *bis* y 197 en el seno del Senado se publicaron en el BOCG de 27 de mayo de 2010. En concreto, en la enmienda nº 13 presentada por el Grupo Parlamentario de Senadores Nacionalistas (GPSN) estaba prevista la eliminación del artículo 31 *bis*, reiterando que sería preciso delimitar las personas a las que se les aplicaría la atenuación de la responsabilidad penal de la persona jurídica una vez se haya cometido el delito, una reforma de la Ley de Enjuiciamiento Criminal en cuanto a imputación y una modificación en el ámbito de las relaciones jurídicas en el proceso, en la línea expuesta por el Grupo Parlamentario Vasco (EAJ-PNV) en su enmienda nº 99 ante el Congreso.

Por su parte, el Grupo Parlamentario Popular en el Senado (GPP) reitera con su enmienda nº 96 la modificación del artículo 31 *bis*, apartado 5, empleando los mismos términos de su enmienda nº 337 ante el Congreso y, por tanto, manifestando el rechazo a la exclusión de los partidos políticos, sindicatos u otras personas jurídicas que presten servicios esenciales a la comunidad, e introduce la enmienda nº 97, relativa a la inclusión de una letra e) en el apartado 4 y un nuevo apartado 4 dentro del artículo 31 *bis* dirigida a incentivar la colaboración de las personas jurídicas con el Estado[184].

[184] En concreto, la modificación propuesta se refiere a la introducción de los siguientes apartados: *"Art 31 bis, 4 e). En el caso de que no concurrieren todas las medidas eficaces para prevenir y descubrir los delitos, se impondrá la pena inferior en uno o dos grados a la señalada por la ley.".*

*"Art 31 bis. 4 bis. Se considera circunstancia eximente de la responsabilidad criminal, si los delitos se hubieran cometido pese al previo*

Finalmente, el Grupo Parlamentario Entesa Catalana de Progrés (GPECP) propuso la supresión del apartado 8 del artículo 197, reiterando los argumentos de la enmienda nº 29, presentada por el Grupo Parlamentario de Esquerra Republicana-Izquieda Unida-Iniciativa per Catalunya-Verds ante el Congreso y relativa a su rechazo del término "grupo", que conllevaba la inclusión de los supuestos de mero acuerdo ocasional para delinquir, propio de la codelincuencia, en el ámbito de la delincuencia organizada.

El Senado acordaba la designación de ponencia para informar sobre el Proyecto y decidía dictaminar sobre el Proyecto en fecha 2 de junio de 2010. En cuanto al Dictamen sobre el Proyecto, en la sesión fueron rechazadas las enmiendas relativas a los citados artículos 31 *bis* y 197, designando miembro de la Comisión de Justicia para la presentación del Dictamen ante el Pleno de la Cámara.

En fecha 9 de junio de 2010 se debatía en el Pleno del Senado el citado Dictamen emitido por la Comisión de Justicia, reiterando el Ministro de Justicia la defensa del Proyecto, con expresa referencia a la tipificación de nuevos delitos como los delitos informáticos y la responsabilidad penal de las personas jurídicas, superando el *societas delinquere non potest* para poder castigar la denominada irresponsabilidad organizada. El Grupo Socialista apoyó el texto, destacando la introducción de la responsabilidad penal de las personas jurídicas en el Código Penal, matizando que el tiempo determinará si

---

*establecimiento por parte de la persona jurídica de medidas eficaces para prevenirlos y descubrirlos*."

la respuesta es acertada, y defendiendo la incorporación de determinados delitos, como los delitos informáticos. La reforma también contaba con el apoyo de Coalición Canaria en lo que respecta a la regulación de la responsabilidad penal de las personas jurídicas, porque de esta forma se aumentaba la seguridad jurídica, y en lo relativo a la introducción de los delitos informáticos.

Al respecto, el Grupo de Senadores Nacionalistas reiteraba su preocupación por la inclusión del artículo 31 *bis*, por cuanto aunque el artículo había sido mejorado en su redacción durante la tramitación parlamentaria, exigiría determinar los sujetos responsables a los que se puede imponer la atenuación de la responsabilidad de las personas jurídicas una vez se ha cometido el delito y se hace precisa una reforma de la Ley de Enjuiciamiento Criminal para extender las garantías procesales a las personas jurídicas.

En el turno en contra, el Grupo Socialista en el Senado volvía a defender la responsabilidad penal de las personas jurídicas y la exclusión de determinadas personas jurídicas como los partidos o los sindicatos por cuanto su disolución podría conllevar problemas de inconstitucionalidad.

El Grupo Parlamentario Mixto reiteraba la preocupación por la introducción de la responsabilidad penal de las personas jurídicas, que exigía una adaptación simultánea de las normas procesales, razón por la cual se pedía una suspensión de su entrada en vigor hasta que se llevara a cabo la necesaria reforma procesal.

Según publicaba el Diario de Sesiones del Senado de fecha 9 de junio de 2010 todas las citadas enmiendas fueron rechazadas, quedando definitivamente aprobado el Proyecto.

Por tanto, a pesar de las enmiendas mencionadas, en fecha 11 de junio de 2010 se publicaba en el BOCG el acuerdo del Pleno del Senado por el que se aprobaba el texto del Proyecto remitido por el Congreso sin introducir modificación alguna.

La reforma del Código Penal operada por la LO 5/2010 fue finalmente publicada en el BOE de 23 de junio de 2010[185], la cual supone su vigesimoséptima reforma, introduciendo por primera vez las conductas de *hacking* en el artículo 197.3 CP, pasando los anteriores apartados 3, 4, 5 y 6 a ser los apartados 4, 5, 6 y 7, y añadiendo un apartado 8, con la siguiente redacción: *"3. 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. 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 impondrá la pena de multa de seis meses a dos años. Atendidas las reglas establecidas en el artículo 66 bis, los jueces y tribunales*

185 Disponible en http://www.boe.es/boe/dias/2010/06/23/pdfs/BOE-A-2010-9953.pdf, consultado el 18 de septiembre de 2016.

*podrán asimismo imponer las penas recogidas en las letras b) a g) del apartado 7 del artículo 33. […] 8. Si los hechos descritos en los apartados anteriores se cometiesen en el seno de una organización o grupo criminales, se aplicarán respectivamente las penas superiores en grado".*

Por tanto, frente a la inicial previsión del Proyecto publicado en el BOCG de 15 de enero de 2007, finalmente fue aprobado un texto en el que se incluían las conductas de mantenimiento no autorizado en el sistema informático, que no estaban previstas en la DM 2005/222/JAI, y los supuestos de responsabilidad de las personas jurídicas, cuya regulación penal era facultativa para los Estados miembros de conformidad con el artículo 8 de la citada norma comunitaria. En consecuencia, el legislador excedía los mínimos fijados en la normativa comunitaria en la materia, en lo que parece un buen intento por llevar a cabo una minuciosa regulación de este fenómeno en el ámbito penal tratando así de dar la mayor cobertura posible a las variantes que puedan surgir con ocasión del acceso a un sistema informático ajeno.

### *4.3.2 La reforma del año 2015.*

A pesar de la reciente introducción de la conducta de *hacking*, en fecha 4 de octubre de 2013 se publicaba en el BOCG un nuevo Proyecto de Ley Orgánica por la que se modifica la Ley Orgánica

10/1995, de 23 de noviembre, del Código Penal[186] y que también afectaba al intrusismo informático en cuanto a sus artículos 31 *bis*, 66 *bis*, 197 *bis* y siguientes. El Proyecto destacaba en su Exposición de Motivos, en relación con el nuevo artículo 31 *bis*, "*una mejora técnica en la regulación de la responsabilidad penal de las personas jurídicas*", "*con la finalidad de delimitar adecuadamente el contenido del «debido control», cuyo quebrantamiento permite fundamentar su responsabilidad penal*" y "*se extiende el régimen de responsabilidad penal a las Sociedades mercantiles Estatales que ejecuten políticas públicas o presten servicios de interés económico general*", dando lugar a un nuevo artículo 31 *bis*, pasando sus anteriores apartados 2 y 3 al nuevo artículo 31 *ter*; se regulaba en el nuevo artículo 31 *quáter* el anterior artículo 31 *bis*.4 y, por último, el artículo 31 *bis*.5 pasaba sustancialmente al artículo 31 *quinquies*, si bien como novedad se citaban las "*Sociedades mercantiles Estatales que ejecuten políticas públicas o presten servicios de interés económico general*", a las que "*les podrán ser impuestas las penas previstas en las letras a) y g) del número 7 del artículo 33*" ("*Multa por cuotas o proporcional*" y/o "*Intervención judicial para salvaguardar los derechos de los trabajadores o de los acreedores*").

En este sentido, la enmienda 320 presentada por el Grupo Parlamentario de IU, ICV-EUiA, CHA: La Izquierda Plural al Proyecto proponía la supresión del artículo 31 *bis* por cuanto se

[186] Texto del Proyecto disponible en http://www.congreso.es/public_oficiales/L10/CONG/BOCG/A/BOCG-10-A-66-1.PDF#page=1, consultado el 18 de septiembre de 2016.

consideraba que "*los problemas político-criminales que plantean las empresas y personas jurídicas*" debían resolverse en el ámbito del artículo 129 CP, careciendo de sentido "*establecer una duplicidad de regulaciones como la mantenida por el actual artículo 31 bis, ni por los nuevos artículos 31 bis, 31 ter, 31 quáter y 31 quinquies*", mientras que la enmienda 416 del Grupo Parlamentario Catalán (Convergència i Unió) pretendía introducir en el listado del artículo 31 *quinquies*, como entidades también excluidas, "*las Corporaciones de Derecho Público*". Las enmiendas fueron rechazadas[187].

Por otra parte, el Proyecto también modificaba el artículo 66 *bis*.2ª CP, al introducir, en relación a las penas que cita anteriormente, que "*Cuando la responsabilidad de la persona jurídica, en los casos previstos en la letra b) de apartado 1 del artículo 31 bis, derive de un incumplimiento de los deberes de supervisión, vigilancia y control que no tenga carácter grave, estas penas tendrán en todo caso una duración máxima de dos años"*. En relación con esta redacción, la enmienda 218 del Grupo Parlamentario Vasco (EAJ-PNV) pretendía subir el límite a los tres años porque "*se corresponde con el injusto penal de la persona jurídica*" y la enmienda 632 presentada por el Grupo Parlamentario Socialista pretendía la supresión de la nueva

[187] Las enmiendas al Proyecto publicado el 4 de octubre de 2013 en el BOCG se encuentran disponibles en http://www.congreso.es/portal/page/portal/Congreso/PopUpCGI?CMD=VERLST&CONF=BRSPUB.cnf&BASE=PU10&PIECE=PU10&DOCS=1-1&FMT=PUWTXDTT.fmt&OPDEF=Y&QUERY=BOCG-10-A-66-2.CODI, consultado el 18 de septiembre de 2016.

regla 2ª del artículo 66 *bis* "*En coherencia con la enmienda al artículo 31 bis*". Ambas enmiendas fueron rechazadas.

Por último, en relación con el nuevo artículo 197 *bis* CP, la LO 1/2015 destacaba en su Exposición de motivos la obligación de transponer la Directiva 2013/40/UE antes del 4 de septiembre de 2015, motivando el nuevo precepto en sustitución del anterior artículo 197.3.

La modificación del artículo 197.3 y la redacción del nuevo artículo 197 *bis* vienen precedidos de cinco enmiendas (823, 824, 825, 826 y 827[188]) introducidas en fecha 10 de diciembre de 2014, que fueron directamente aprobadas por el Congreso de los Diputados con la justificación de que la Directiva 2013/40/UE "*fue aprobada publicada* (sic) *en agosto de 2013, cuando el anteproyecto de reforma ya había sido aprobado por el Gobierno y era inminente su aprobación como Proyecto de Ley*", el plazo de transposición de la Directiva 2013/40/UE vencía el 4 de septiembre de 2015 y considerando que "*se introduce una separación nítida entre los supuestos de revelación de datos que afectan directamente a la intimidad personal, y el acceso a otros datos o informaciones que pueden afectar a la privacidad pero que no están referidos directamente a la intimidad personal*".

[188] Enmiendas disponibles en http://www.congreso.es/portal/page/portal/Congreso/PopUpCGI?CMD=VERLST&CONF=BRSPUB.cnf&BASE=PU10&PIECE=PUWD&DOCS=1-1&FMT=PUWTXDTU.fmt&OPDEF=Y&QUERY=BOCG-10-A-66-2.CODI., consultado el 18 de septiembre de 2016.

La enmienda 823 modificaba el artículo 197 del CP, destipificando en este precepto las conductas de *hacking*, que pasaban a incluirse en un nuevo artículo 197 *bis* 1, conforme a la enmienda 824. Además, la enmienda 823 suponía que las conductas de difundir, revelar o ceder a terceros los datos o hechos descubiertos o las imágenes captadas, antes reguladas en el artículo 197.4 CP y referidas también al *hacking*, se incluyeran en su nuevo artículo 197.3 y en relación sólo a los supuestos del artículo 197, apartados 1 o 2; los casos de realización de los hechos descritos en los tipos del artículo 197, apartados 1 y 2 CP, por personas encargadas o responsables de ficheros, soportes, archivos o registros, pasaban a destipificarse de su artículo 197.5 para incluirse en el artículo 197.4; de igual forma, la afectación a datos personales que revelen la ideología, religión, creencias, salud, origen racial o vida sexual, o cuando la víctima fuera menor de edad o persona incapaz, pasaba del artículo 197.6, donde afectaba también al *hacking*, a tipificarse en el artículo 197.5 y con referencia tan sólo a las conductas anteriores de ese mismo precepto, es decir, ahora se excluía la agravante en relación con el *hacking*; el ánimo de lucro, antes tipificado en el artículo 197.7 CP y en referencia a las conductas del artículo 197, pasaba a su artículo 197.6, igualmente relacionado con los supuestos de ese artículo y, por tanto, excluyendo esa agravante en relación con el *hacking.* Por último, se incluía como novedad en el artículo 197.7 CP los tipos de difusión, revelación o cesión no autorizada a terceros de imágenes o grabaciones de una persona obtenidas con su anuencia y menoscabando gravemente la intimidad personal de esa persona.

Como recuerda MANZANARES SAMANIEGO[189], las citadas enmiendas fueron aceptadas en el Congreso de los Diputados sin los dictámenes previos del Consejo Fiscal, CGPJ y Consejo de Estado. La explicación se debe a que la Directiva 2013/40/UE fue publicada en el DOUE de 14 de agosto de 2013 y el nuevo artículo es consecuencia de las citadas enmiendas del Grupo Popular aceptadas en el Congreso de los Diputados, posteriores a los citados dictámenes, razón por la cual el nuevo texto del artículo 197 *bis* no pudo ser incluido en los informes.

Por tanto, el Anteproyecto de octubre de 2012[190] no contiene referencia alguna a la modificación de las conductas de *hacking* en el Código Penal finalmente introducidas con la LO 1/2015, ni obviamente el Consejo Fiscal pudo pronunciarse en su Informe al Anteproyecto emitido en fecha 8 de enero de 2013[191], ni tampoco el

---

189 MANZANARES SAMANIEGO, J.L., *La reforma del Código penal …*, *cit*., nota 170, p. 201.

190 "*Anteproyecto de Ley Orgánica por la que se modifica la Ley Orgánica 10/1995, de 23 de noviembre, del Código penal*", disponible en http://www.mjusticia.gob.es/cs/Satellite/Portal/1292358725605?blobheader=application%2Fpdf&blobheadername1=Content-Disposition&blobheadername2=Medios&blobheadervalue1=attachment%3B+filename%3DAnteproyecto_de_Ley_de_Reforma_del_Codigo_Penal.pdf&blobheadervalue2=1288777317612, consultado el 18 de septiembre de 2016.

191 "*Informe del Consejo Fiscal al Anteproyecto de Ley Orgánica por la que se modifica la Ley Orgánica 10/1995, de 24 de noviembre* (sic), *del Código Penal*", disponible en https://www.fiscal.es/fiscal/PA_WebApp_SGNTJ_NFIS/descarga/INFORME_ANTEPROYECTO_CP_2012_8-enero-2013.pdf?idFile=ab37a28b-9fbc-4af5-b2b3-3b14c1826623, consultado el 18 de septiembre de 2016.

Informe del CGPJ de 16 de enero de 2013[192] o el Dictamen del Consejo de Estado de fecha 27 de junio de 2013[193] la mencionan.

De esta forma, la modificación del artículo 197 del Código Penal, en cuyo apartado 3 se tipificaban desde la LO 5/2010 las conductas de *hacking*, y el nuevo artículo 197 *bis* 1 fueron directamente introducidos con las enmiendas propuestas por el Grupo Popular en el Congreso de los Diputados.

El texto del artículo 197 *bis* 1 introducido con la enmienda 824 ha sido el finalmente aprobado sin ninguna modificación: "*El que por cualquier medio o procedimiento, vulnerando las medidas de seguridad establecidas para impedirlo, y sin estar debidamente autorizado, acceda o facilite a otro el acceso al conjunto o una parte de un sistema de información o se mantenga en él 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*". Por su parte, el artículo 197 *ter*, relativo a facilitar la comisión del delito, que no estaba tipificado con anterioridad a la LO 1/2015, fue introducido con la enmienda 825; el artículo 197 *quater*, introducido con la enmienda 826, en relación a la comisión en organizaciones o grupos criminales,

---

[192] Informe disponible en http://www.poderjudicial.es/cgpj/es/Poder-Judicial/Consejo-General-del-Poder-Judicial/Actividad-del-CGPJ/Informes/Informe-al-Anteproyecto-de-Ley-Organica-por-la-que-se-modifica-la-Ley-Organica-10-1995--de-23-de-noviembre--del-Codigo-Penal, consultado el 18 de septiembre de 2016.

[193] Dictamen disponible en https://www.boe.es/buscar/doc.php?id=CE-D-2013-358, consultado el 18 de septiembre de 2016.

supone su destipificación del artículo 197.8 CP, si bien sigue refiriéndose a las conductas de los artículos anteriores; y el artículo 197 *quinquies*, cuando la responsabilidad recaiga sobre una persona jurídica, acompañado con la enmienda 827, supone el abandono de su regulación en el anterior artículo 197.3 CP, aunque sigue manteniendo su referencia a los delitos comprendidos en los artículos anteriores.

Las citadas enmiendas 824, 825, 826 y 827 por las que finalmente se introdujeron los artículos 197 *bis*, 197 *ter*, 197 *quater* y 197 *quinquies* en el Código penal tienen idéntica justificación, "*superar las limitaciones de la regulación vigente para ofrecer respuesta a la delincuencia informática en el sentido de la Directiva 2013/40/UE"* y fueron aceptadas en el Informe de la Ponencia de fecha 13 de enero de 2015[194], proponiendo a la Comisión su inclusión, que fue llevada a cabo con su Dictamen de fecha 16 de enero de 2015[195], si bien en el Dictamen se introducen algunas modificaciones

[194] Informe disponible en http://www.congreso.es/portal/page/portal/Congreso/PopUpCGI?CMD=VERLST&BASE=pu10&FMT=PUWTXDTS.fmt&DOCS=1-1&DOCORDER=LIFO&QUERY=%28BOCG-10-A-66-3.CODI.%29#%28P%C3%A1gina1%29, consultado el 18 de septiembre de 2016.

[195] Dictamen disponible en http://www.congreso.es/portal/page/portal/Congreso/PopUpCGI?CMD=VERLST&BASE=pu10&FMT=PUWTXDTS.fmt&DOCS=1-1&DOCORDER=LIFO&QUERY=%28BOCG-10-A-66-4.CODI.%29#%28P%C3%A1gina1%29, consultado el 18 de septiembre de 2016.

en los artículos 197 *quáter*[196] y 197 *quinquies*[197] con respecto al contenido de las enmiendas 826 y 827.

El texto del Proyecto fue aprobado por el Pleno del Congreso de los Diputados el 21 de enero de 2015[198], tuvo entrada en el Senado en fecha 29 de enero de 2015[199], y en fecha 10 de febrero de 2015 se

---

[196] Mientras la enmienda 826 proponía como texto del artículo 197 *quáter* "*Si los hechos descritos en los artículos anteriores se hubieran cometido en el seno de una organización o grupo criminales, se aplicarán respectivamente las penas superiores en grado*", el Dictamen lo modifica introduciendo el siguiente texto: "*Si los hechos descritos en este Capítulo se hubieran cometido en el seno de una organización o grupo criminal, se aplicarán respectivamente las penas superiores en grado*", texto que sería finalmente aprobado.

[197] La enmienda 826 proponía como texto del artículo 197 *quinquies* "*Cuando de acuerdo con lo establecido en el artículo 31 bis una persona jurídica sea responsable de los delitos comprendidos en los artículos anteriores, se le impondrá la pena de multa de seis meses a dos años. 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*", el Dictamen modifica introduce el siguiente texto: "*Cuando de acuerdo con lo establecido en el artículo 31 bis una persona jurídica sea responsable de los delitos comprendidos en los artículos 191, 197 bis y 197 ter, se le impondrá la pena de multa de seis meses a dos años. 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*", texto que sería finalmente aprobado.

[198] Texto de la aprobación disponible en http://www.congreso.es/portal/page/portal/Congreso/PopUpCGI?CMD=VERLST&BASE=pu10&FMT=PUWTXDTS.fmt&DOCS=1-1&DOCORDER=LIFO&QUERY=%28BOCG-10-A-66-5.CODI.%29#%28P%C3%A1gina1%29, consultado el 18 de septiembre de 2016.

[199] Texto disponible en http://www.congreso.es/portal/page/portal/Congreso/PopUpCGI?CMD=VE

introducen con motivo de "*corrección técnica*" las enmiendas 975 y 976[200] del Grupo Popular en el Senado, que de nuevo afectan al artículo 197 (si bien este artículo ya no contiene referencia a las conductas de *hacking*), los artículos 197 *ter*[201] y 197 *quinquies*[202].

---

RLST&BASE=pu10&FMT=PUWTXDTS.fmt&DOCS=1-1&DOCORDER=LIFO&QUERY=%28BOCG_D_10_465_3148.CODI.%29#%28P%C3%A1gina2%29, consultado el 18 de septiembre de 2016.

[200] Enmiendas disponibles en http://www.congreso.es/portal/page/portal/Congreso/PopUpCGI?CMD=VERLST&BASE=pu10&FMT=PUWTXDTS.fmt&DOCS=1-1&DOCORDER=LIFO&QUERY=%28BOCG_D_10_475_3158.CODI.%29#%28P%C3%A1gina85%29 consultado el 18 de septiembre de 2016.

[201] El texto recibido por el Senado establecía en su artículo 197 *ter* "*Será castigado con una pena de prisión de seis meses a dos años o multa de tres a dieciocho meses el que, sin estar debidamente autorizado, produzca, adquiera para su uso, importe o, de cualquier modo, facilite a terceros, con la intención de facilitar la comisión de alguno de los delitos a que se refieren los apartados 1 y 2 del artículo 197 o el artículo 197 bis: a) un programa informático, concebido o adaptado principalmente para cometer alguno de los delitos a que se refieren los dos artículos anteriores; o b) una contraseña de ordenador, un código de acceso o datos similares que permitan acceder a la totalidad o a una parte de un sistema de información"*, y el nuevo texto añadido por "*corrección técnica*" con la enmienda 975 del Grupo Popular introducía que "*Será castigado con una pena de prisión de seis meses a dos años o multa de tres a dieciocho meses el que, sin estar debidamente autorizado, produzca, adquiera para su uso, importe o, de cualquier modo, facilite a terceros, con la intención de facilitar la comisión de alguno de los delitos a que se refieren los apartados 1 y 2 del artículo 197 o el artículo 197 bis: a) un programa informático, concebido o adaptado principalmente para cometer dichos delitos alguno de los delitos a que se refieren los dos artículos anteriores; o b) una contraseña de ordenador, un código de acceso o datos similares que permitan acceder a la totalidad o a una parte de un sistema de información*".

[202] Mientras el texto recibido en el Senado establecía en el artículo 197 *quinquies* "*Cuando de acuerdo con lo establecido en el artículo 31 bis una*

El Informe de la Ponencia del Senado fue emitido en fecha 23 de febrero de 2015[203], donde se modifica el apartado a) del artículo 197 *ter*, para incluir "*un programa informático, concebido o adaptado principalmente para cometer dichos delitos*", conforme a la enmienda 975, y se corrige la errata de la enmienda 976 al artículo 197 *quinquies*, relacionando el precepto con los *"artículos 1971, 197 bis y 197 ter"*, para referirlo a los "*artículos 197, 197 bis y 197 ter*".

El Dictamen de la Comisión de Justicia del Senado fue emitido en fecha 3 de marzo de 2015[204] y el texto fue aprobado por el Pleno del Senado el 11 de marzo de 2015[205] y la aprobación definitiva del

---

*persona jurídica sea responsable de los delitos comprendidos en los artículos 191, 197 bis y 197 ter, se le impondrá la pena de multa de seis meses a dos años. 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*" con la enmienda 976 el Grupo Popular introduce "*Cuando de acuerdo con lo establecido en el artículo 31 bis una persona jurídica sea responsable de los delitos comprendidos en los artículos 1971* (sic)*, 197 bis y 197 ter, se le impondrá la pena de multa de seis meses a dos años. 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*".

[203] Informe disponible en http://www.congreso.es/portal/page/portal/Congreso/PopUpCGI?CMD=VERLST&BASE=pu10&FMT=PUWTXDTS.fmt&DOCS=1-1&DOCORDER=LIFO&QUERY=%28BOCG_D_10_481_3237.CODI.%29#%28P%C3%A1gina3%29, consultado el 18 de septiembre de 2016.

[204] Dictamen disponible en http://www.congreso.es/portal/page/portal/Congreso/PopUpCGI?CMD=VERLST&BASE=pu10&FMT=PUWTXDTS.fmt&DOCS=1-1&DOCORDER=LIFO&QUERY=%28BOCG_D_10_485_3263.CODI.%29#%28P%C3%A1gina6%29, consultado el 18 de septiembre de 2016.

[205] Texto disponible en

Proyecto por el Congreso de los Diputados tuvo lugar el 26 de marzo de 2015[206], siendo finalmente publicada la nueva LO 1/2015 en el BOE de 31 de marzo de 2015[207], a la que se hace referencia en los siguientes capítulos.

En consecuencia, en apenas dos años desde la entrada en vigor de la reforma de la LO 5/2010, el legislador ya había presentado un nuevo Proyecto para modificar de nuevo del Código Penal. Su texto inicial no establecía la modificación de las conductas de *hacking*, lo cual parece mínimamente lógico porque apenas había dado tiempo a su aplicación. Sin embargo, en fecha 10 de diciembre de 2014 y una vez emitidos los dictámenes del Consejo Fiscal, CGPJ y Consejo de Estado, se presentaban y se aprobaban las enmiendas introducidas con ocasión de la Directiva 2013/40/UE, sobre las que por tanto no pudieron pronunciarse los citados organismos y que daban un vuelco al artículo 197 CP en un intento por separar esos comportamientos

---

http://www.congreso.es/portal/page/portal/Congreso/PopUpCGI?CMD=VERLST&BASE=pu10&FMT=PUWTXDTS.fmt&DOCS=1-1&DOCORDER=LIFO&QUERY=%28BOCG_D_10_493_3340.CODI.%29#%28P%C3%A1gina2%29, consultado el 18 de septiembre de 2016.

[206] Texto disponible en http://www.congreso.es/portal/page/portal/Congreso/PopUpCGI?CMD=VERLST&BASE=pu10&FMT=PUWTXDTS.fmt&DOCS=1-1&DOCORDER=LIFO&QUERY=%28BOCG-10-A-66-7.CODI.%29#%28P%C3%A1gina1%29, consultado el 18 de septiembre de 2016.

[207] Texto de la LO 1/2015, publicado en el BOE nº 77, de 31 de marzo de 2015, disponible en https://www.boe.es/diario_boe/txt.php?id=BOE-A-2015-3439, consultado el 18 de septiembre de 2016.

respecto a los delitos contra la intimidad, pero manteniendo estas conductas en el mismo capítulo.

Por tanto, se trata de una reforma que en lo que afecta al *hacking* fue realizada sin los citados dictámenes jurídicos, que se justificaba según sus enmiendas en que vencía el plazo de transposición de la citada Directiva y en tratar de desvincularlo de las conductas del artículo 197 CP, llevándolo a un precepto propio. Sin embargo, la reforma sigue manteniendo esos delitos en el mismo capítulo de los delitos contra la intimidad y crea todo un entramado de conductas y circunstancias en torno a los artículos 197 y 197 *bis* de difícil interpretación, a buen seguro provocado por las prisas por legislar sobre la materia. Todo ello apunta a un necesario nuevo cambio legislativo que al tercer intento aporte cierto orden y autonomía a las conductas de *hacking* respecto a los delitos contra la intimidad.

# CAPÍTULO II.

# BREVE REFERENCIA AL DELITO DE *HACKING* EN EL DERECHO COMPARADO EUROPEO.

## *1. INTRODUCCIÓN.*

En el ámbito de las legislaciones penales europeas el punto de partida para la regulación de las conductas de *hacking* se encuentra en el citado Convenio Europeo sobre Cibercriminalidad, en cuyos artículos 2 a 6 se imponía a los Estados miembros la obligación de regular en el ámbito penal los "*Delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos*". La DM 2005/222, emitida por el Consejo de la Unión Europea en fecha 24 de febrero de 2005, relativa a los ataques de los que son objeto los sistemas de información, es la norma europea que, como señala DE LA MATA[208], mejor desarrolla en buena parte el citado Convenio, imponiendo a los Estados que castiguen penalmente el acceso intencionado no autorizado a un sistema de información (artículo 2) y la perturbación de sistemas informáticos (artículo 3). A esta Decisión Marco le ha sustituido, tras varias Comunicaciones, la Directiva 2013/40/UE, que se ocupa del "*Acceso ilegal a los sistemas de información*" en su artículo 3, tal y como se ha ido explicando en el Capítulo anterior.

Como consecuencia de esta normativa europea, a fecha del presente trabajo han sido numerosos los países que han incluido en su legislación penal las conductas de instrusismo informático. Así ha sucedido con los países de nuestro entorno en el ámbito de la Unión

[208] DE LA MATA BARRANCO, N. J., *Derecho penal europeo y legislación española: las reformas del Código penal*, Ed. Tirant lo Blanch, Valencia, 2015, p. 89.

europea, es decir, actualmente, Austria (1995), Bélgica (1958), Bulgaria (2007), Chipre (2004), Croacia (2013), República Checa (2004), Dinamarca (1973), Estonia (2004), Finlandia (1995), Francia (1958), Alemania (1958), Grecia (1981), Hungría (2004), Irlanda (1973), Italia (1958), Letonia (2004), Lituania (2004), Luxemburgo (1958), Malta (2004), Países Bajos (1958), Polonia (2004), Portugal (1986), Rumanía (2007), Eslovaquia (2004), Eslovenia (2004), Suecia (1995) y Reino Unido (1973)[209].

Sin embargo, a pesar de compartir el marco normativo europeo, la regulación del delito de *hacking* no ha sido igual en todos los casos, pudiendo clasificarse en los siguientes grupos:

(i) Los países que regulan en normas penales especiales los delitos informáticos.

(ii) Los que tipifican el *hacking* en un título o capítulo propio y diferenciado dentro de su Código penal.

(iii) Los países que, como España, regulan el intrusismo informático junto a otros delitos, es decir, los restantes Estados citados.

Atendida la citada clasificación, se exponen brevemente a continuación las mencionadas legislaciones europeas con sus correspondientes peculiaridades.

[209] Los países de la Unión Europea y el año de ingreso en la UE que se indica entre paréntesis están disponibles en http://europa.eu/about-eu/countries/index_es.htm, consultado el 12 de enero de 2017.

## 2. *PAÍSES QUE REGULAN LOS DELITOS INFORMÁTICOS EN NORMAS PENALES ESPECIALES.*

Entre las legislaciones europeas donde se ha optado por regular el *hacking* de forma diferenciada de otros delitos, incluyéndolo en normas penales especiales, se encuentran las de Chipre, Portugal y Reino Unido. A esta normativa especial se refieren los siguientes subepígrafes, con especial mención a sus diferencias con la regulación española, que será analizada en los siguientes Capítulos.

### *2.1 Chipre.*

La Ley que ratifica la Convención del Consejo de Europa contra la delincuencia a través de Internet, de fecha 30 de abril de 2004[210], dedica una parte primera a disposiciones generales. Entre ellas, su artículo 2 incluye conceptos, definiendo qué se entiende por sistema informático de forma similar al artículo 1 del Convenio Europeo sobre Cibercriminalidad, e incorporando además la definición de "sin autorización", que comprende el acceso a un

[210] Ley disponible en https://www.google.es/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&uact=8&ved=0ahUKEwjaztmDvcfLAhWCdx4KHQMCCl8QFggdMAA&url=http%3A%2F%2Fwww.police.gov.cy%2Fpolice%2Fpolice.nsf%2FAll%2F7CF46652A4E4D9BDC2257A3A003281B2%2F%24file%2Fnomosdiadiktyou.doc&usg=AFQjCNFjsQuaein0zz8HrVoz_EqYp9CKjg, consultado el 12 de enero de 2017.

sistema informático o parte del mismo, o la intromisión, no autorizados por el propietario o titular de otro derecho sobre el sistema o prohibidos por las disposiciones de esta Ley[211].

La parte segunda de la Ley incorpora los delitos contra la confidencialidad, la integridad de los datos y la disponibilidad y los sistemas informáticos. Entre ellos, el artículo 4 castiga al sujeto que intencionadamente y sin derecho acceda a todo o parte de un sistema informático, vulnerando las medidas de seguridad establecidas[212].

Por tanto, al igual que el Código Penal español, hay una expresa referencia a la vulneración de medidas de seguridad que exige el artículo 3 de la Directiva 2013/40/UE, pero no al mantenimiento en el sistema de información al que se refiere también el artículo 197 *bis* del Código Penal, siendo de destacar el establecimiento de un precepto específico para las definiciones, siguiendo la normativa internacional, si bien el legislador chipriota ha dado un paso más incorporando conceptos como el relativo a la autorización, no

---

211 Las definiciones de sistema informático y sin autorización se encuentran en el artículo 2 de la citada Ley: *""Σύστημα υπολογιστή" σημαίνει συσκευή ή ομάδα συσκευών που είναι εσωτερικά συνδεδεμένες μεταξύ τους ή συνδεδεμένες συσκευές, οι οποίες επεξεργάζονται αυτόματα δεδομένα, με τη χρήση προγράμματος.*
*«Χωρίς δικαίωμα» σημαίνει πρόσβαση ή παρεμβολή μη εξουσιοδοτημένης από τον ιδιοκτήτη ή άλλο δικαιούχο του συστήματος υπολογιστή ή μέρος αυτού, ή απαγορευμένη δυνάμει των διατάξεων του παρόντος Νόμου*".

212 El artículo 4 de la Ley establece: "*Όποιος με πρόθεση και χωρίς δικαίωμα εισέρχεται στο σύνολο ή μέρος συστήματος ηλεκτρονικών υπολογιστών, παραβιάζοντας τα μέτρα ασφάλειας διαπράττει αδίκημα που τιμωρείται με φυλάκιση που δεν υπερβαίνει τα πέντε έτη ή με χρηματική ποινή που δεν υπερβαίνει τις 34,172 ευρώ ή και με τις δύο ποινές*".

contemplados en los instrumentos internacionales.

Por su parte, el artículo 8 castiga con iguales penas al sujeto que intencionadamente y sin derecho produzca, venda, procure, importe, distribuya o de cualquier otro modo realice un dispositivo, incluido un programa informático, diseñado o adaptado para cometer el delito del artículo 4, o un código de acceso o dato similar por el cual todo o parte del sistema informático llega a ser accesible para su uso en el citado delito, de forma similar al artículo 197 *ter* introducido en el Código español tras la reforma de la LO 1/2015, que veremos en el Capítulo IV. También se establecen las mismas penas para el sujeto que intencionadamente y sin derecho posea algunos de los citados dispositivos o datos para cometer los delitos del artículo 4[213].

---

[213] El artículo 8 dispone: "*(1) Απαγορεύεται η με πρόθεση και χωρίς δικαίωμα παραγωγή, πώληση, προμήθευση προς χρήση, εισαγωγή, διανομή ή με άλλο τρόπο διάθεση -*

*(α) Μιας συσκευής συμπεριλαμβανομένου προγράμματος υπολογιστή που έχει σχεδιαστεί ή προσαρμοστεί πρωτίστως με σκοπό τη διάπραξη οποιουδήποτε από τα αδικήματα που προβλέπονται στις διατάξεις των άρθρων 4 - 7 του παρόντος Νόμου.*

*(β) κλειδάριθμου ηλεκτρονικού υπολογιστή, κωδικού πρόσβασης ή παρόμοια δεδομένα με τα οποία ολόκληρο ή μέρος συστήματος υπολογιστή γίνεται προσβάσιμο με σκοπό να χρησιμοποιηθεί για τη διάπραξη οποιουδήποτε από τα αδικήματα που προβλέπονται στις διατάξεις των άρθρων 4 - 7του παρόντος Νόμου.*

*(2) Απαγορεύεται η με πρόθεση και χωρίς δικαίωμα κατοχή των αναφερομένων στις παραγράφους (α) και (β) του εδαφίου (1) του παρόντος άρθρου, με σκοπό να χρησιμοποιηθούν για τη διάπραξη οποιουδήποτε από τα αδικήματα που καθορίζονται στα άρθρα 4 – 7 του παρόντος Νόμου.*

*΄Οποιος ενεργεί κατά παράβαση των εδαφίων (1) και (2) του παρόντος άρθρου διαπράττει αδίκημα που τιμωρείται με φυλάκιση που δεν*

Por último, su artículo 13 fija las penas para el que intencionadamente asista o incite a la comisión de los delitos del artículo 4[214], y el artículo 14 establece la responsabilidad de las personas jurídicas[215], supuesto previsto en el artículo 197 *quinquies* del Código español tras la reforma de la LO 1/2015, si bien en el caso chipriota pudiendo dirigir el procedimiento contra la empresa o contra todos o cualquiera de las personas físicas encargadas de su gestión.

Con las salvedades citadas, se observa por tanto un cierto paralelismo entre algunas de las conductas reguladas en la mencionada Ley y las introducidas en el Código español por la LO 1/2015 en esta materia. Sin embargo, es de destacar el punto de partida chipriota, que es el establecimiento de una ley especial propia para la regulación de los delitos informáticos a través de Internet, lo

---

*υπερβαίνει τα πέντε έτη ή με χρηματική ποινή που δεν υπερβαίνει τις 34,172 ευρώ ή και με τις δύο ποινές*".

214 Artículo 13: "*΄Οποιος με πρόθεση αποπειράται, συνδράμει ή υποκινεί τη διάπραξη οποιουδήποτε από τα αδικήματα που προβλέπονται στις διατάξεις των άρθρων 4 – 12 του παρόντος Νόμου διαπράττει αδίκημα που τιμωρείται με φυλάκιση που δεν υπερβαίνει τα πέντε έτη ή με χρηματική ποινή μέχρι 34,172 ευρώ ή και με τις δύο ποινές".*

215 Artículo 14: "*Τηρουμένων των διατάξεων οποιουδήποτε άλλου Νόμου, που εφαρμόζεται στη Δημοκρατία αναφορικά με την ευθύνη νομικών προσώπων, για οποιαδήποτε πράξη τους, η οποία συνιστά ποινικό αδίκημα κατά παράβαση των διατάξεων του παρόντος Νόμου, φέρουν ευθύνη για το αδίκημα, εκτός από τα ίδια τα νομικά πρόσωπα-*

*(α) ΄Ολα τα μέλη του διοικητικού ή διαχειριστικού συμβουλίου ή της επιτροπής που διαχειρίζεται τις υποθέσεις των νομικών προσώπων·*

*(β) ο γενικός διευθυντής ή ο διευθυντής ή ο διευθύνων σύμβουλος των νομικών προσώπων,*

*και η ποινική δίωξη για το αδίκημα μπορεί να στραφεί εναντίον της εταιρείας και εναντίον όλων ή οποιουδήποτε από τα πιο πάνω πρόσωπα*".

que parece más acorde con el creciente número de casos relativos a estos delitos y sin duda evita la contaminación interpretativa de estos preceptos que se produciría si se hubiera decidido por incluirlos en un mismo título donde se regularan delitos relativos a otros bienes jurídicos, tal y como sucede en el caso español cuando se decidió incluirlos con la LO 5/2010 entre los delitos contra la intimidad y se ha optado por mantenerlos en el mismo título con la LO 1/2015, según se expondrá en el siguiente Capítulo.

### *2.2 Portugal.*

En el ámbito portugués las conductas de *hacking* estaban reguladas en el artículo 7 de la Lei n.° 109/91 de 17 de agosto (Lei da criminalidade Informática)[216], como consecuencia de la

[216] El artículo 7 de la Lei n.° 109/91 de 17 de agosto (Lei da criminalidade Informática) establecía: "*Artigo 7º. Acesso ilegítimo*

*1 - Quem, não estando para tanto autorizado e com a intenção de alcançar, para si ou para outrem, um beneficio ou vantagens ilegítimos, de qualquer modo aceder a um sistema ou rede informáticos será punido com pena de prisão até 1 ano ou com pena de multa até 120 dias.*

*2 - A pena será a de prisão até três anos ou multa se o acesso for conseguido através de violação de regras de segurança.*

*3 - A pena será a de prisão de um a cinco anos quando:*

*a) Através do acesso, o agente tiver tomado conhecimento de segredo comercial ou industrial ou de dados confidenciais, protegidos por lei;*

*b) O beneficio ou vantagem patrimonial obtidos forem de valor consideravelmente elevado.*

*4 - A tentativa é punível.*

Recomendación (89) nº 9, de 13 de septiembre de 1989 del Consejo de Europa[217], regulando los supuestos de acceso no autorizado a un sistema informático o red de ordenadores para obtener un beneficio o ventaja ilegítima. Las penas se incrementaban en los supuestos en que existiera vulneración de medidas de seguridad, anticipando así la previsión del artículo 3 de la Directiva 2013/40/UE, que incluye expresamente la "*violación de una medida de seguridad*", y el castigo era mayor en los supuestos de que se descubrieran secretos comerciales o industriales o datos confidenciales, protegidos legalmente, o si se obtiene un beneficio considerablemente alto, estando prevista en el mismo precepto la tentativa.

La citada ley incluía definiciones a los efectos de estas conductas siguiendo el modelo del Convenio Europeo sobre Cibercriminalidad, la Decisión Marco 2005/222/JAI y la Directiva 2013/30/UE. Entre esas definiciones, la ley portuguesa establecía las

---

*5 - Nos casos previstos nos nºs 1, 2 e 4 o procedimento penal depende de queixa*.". Disponible en http://www.pgdlisboa.pt/leis/lei_mostra_articulado.php?nid=151&tabela=lei_velhas&nversao=1&so_miolo=, consultado el 12 de enero de 2017.

[217] La Recomendación R (89) 9 de 13 de septiembre de 1989 disponía en su punto 1: "*Recommande aux gouvernements des Etats membres: 1. De tenir compte, lorsqu'ils réviseront leur législation ou en prépareront une nouvelle, du rapport sur la criminalité en relation avec l'ordinateur, élaboré par le Comité européen pour les problèmes criminels, et, en particulier, des príncipes directeurs pour les législateurs nationaux;"*, disponible en https://www.google.es/search?q=Recomendación+núm.+R+(89)+9+sobre+delitos+informáticos&ie=utf-8&oe=utf-8&gws_rd=cr&ei=kCtDVv_2EMWtaa2cjqAI#q=conseil+europe+R+(89)+9, consultado el 12 de enero de 2017.

relativas a red informática, sistema o programa informático en su artículo 1[218].

Sin embargo, la norma fue derogada por la Lei n.º 109/2009, de 15 de septiembre, de transposición de la DM 2005/222/JAI y el Convenio Europeo sobre Cibercriminalidad. La citada Ley 109/2009 dedica su artículo 2 a las definiciones relativas a estas conductas, incluyendo la definición de sistema informático en la línea de la mencionada normativa internacional[219] y se ocupa del acceso ilegítimo a un sistema informático en el artículo 6[220].

---

[218] En este sentido, mientras el artículo 1 del Convenio Europeo sobre Cibercriminalidad define en su artículo 1 "*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*", en el artículo 2 de la Lei n.° 109/91 de 17 de Agosto portuguesa se establecía como "*b) Sistema informático - um conjunto constituído por um ou mais computadores, equipamento periférico e suporte lógico que assegura o processamento de dados;*".

[219] El artículo 2 de Lei n.º 109/2009, de 15 de setembro, define "*a) «Sistema informático», qualquer dispositivo ou conjunto de dispositivos interligados ou associados, em que um ou mais de entre eles desenvolve, em execução de um programa, o tratamento automatizado de dados informáticos, bem como a rede que suporta a comunicação entre eles e o conjunto de dados informáticos armazenados, tratados, recuperados ou transmitidos por aquele ou aqueles dispositivos, tendo em vista o seu funcionamento, utilização, protecção e manutenção*". Ley disponible en http://www.pgdlisboa.pt/leis/lei_mostra_articulado.php?nid=1137&tabela=leis, consultado el 12 de enero de 2017.

[220] "*Artigo 6.º. Acesso ilegítimo.*

*1 - Quem, sem permissão legal ou sem para tanto estar autorizado pelo proprietário, por outro titular do direito do sistema ou de parte dele, de qualquer modo aceder a um sistema informático, é punido com pena de*

En la regulación del *hacking*, el nuevo precepto castiga al que sin estar autorizado por su titular acceda a un sistema informático, imponiendo iguales penas al que facilita datos informáticos para la comisión del delito. Las penas son superiores si se vulneran medidas de seguridad, llegando hasta los 5 años cuando se descubren secretos comerciales o industriales o datos confidenciales, protegidos legalmente, o si se obtiene un beneficio considerablemente alto, estando prevista en el mismo precepto la tentativa.

Por tanto, la normativa portuguesa se encuentra en la línea normativa internacional, emitida incluso con anterioridad a ese conjunto de normas, con una regulación más detallada de las conductas de *hacking* que la normativa española aunque sin incluir los supuestos de permanencia no autorizada dentro del sistema

---

*prisão até 1 ano ou com pena de multa até 120 dias.*

*2 - Na mesma pena incorre quem ilegitimamente produzir, vender, distribuir ou por qualquer outra forma disseminar ou introduzir num ou mais sistemas informáticos dispositivos, programas, um conjunto executável de instruções, um código ou outros dados informáticos destinados a produzir as acções não autorizadas descritas no número anterior.*

*3 - A pena é de prisão até 3 anos ou multa se o acesso for conseguido através de violação de regras de segurança.*

*4 - A pena é de prisão de 1 a 5 anos quando:*

*a) Através do acesso, o agente tiver tomado conhecimento de segredo comercial ou industrial ou de dados confidenciais, protegidos por lei; ou*

*b) O benefício ou vantagem patrimonial obtidos forem de valor consideravelmente elevado.*

*5 - A tentativa é punível, salvo nos casos previstos no n.º 2.*

*6 - Nos casos previstos nos n.os 1, 3 e 5 o procedimento penal depende de queixa*.".

informático. Es destacable la regulación de los delitos informáticos en una ley penal especial, evitando los problemas de la ubicación sistemática de estos delitos, y el intento del legislador por facilitar la labor interpretativa introduciendo las definiciones previas de los elementos de estos delitos.

### *2.3 Reino Unido.*

En el ámbito del Reino Unido, la Ley de abusos informáticos de 29 de junio de 1990[221] regula en su sección 1[222] el acceso no

[221] Ley disponible en su texto original en http://www.legislation.gov.uk/ukpga/1990/18/pdfs/ukpga_19900018_en.pdf, y con sus reformas en http://www.legislation.gov.uk/ukpga/1990/18, consultado el 12 de enero de 2017.

[222] La sección 1, tras las reformas llevadas a cabo por la "*Police and Justice Act 2006*" y el "*Serious Crime Act 2015*", establece: "*Unauthorised access to computer material.*

*(1)A person is guilty of an offence if—*

*(a)he causes a computer to perform any function with intent to secure access to any program or data held in any computer [F1, or to enable any such access to be secured] ;*

*(b)the access he intends to secure [F2, or to enable to be secured,] is unauthorised; and*

*(c)he knows at the time when he causes the computer to perform the function that that is the case.*

*(2)The intent a person has to have to commit an offence under this section need not be directed at—*

*(a)any particular program or data;*

*(b)a program or data of any particular kind; or*

*(c)a program or data held in any particular computer.*

*[F3(3)A person guilty of an offence under this section shall be liable—*

autorizado a material informático, castigando al sujeto que provoca en un ordenador cualquier función para asegurar el acceso a cualquier programa o datos contenidos en un ordenador o para habilitar el acceso, cuando el acceso no está autorizado, y además el sujeto es consciente de la función del ordenador en ese momento.

En las conductas previstas en esta sección, se requiere que la intención del sujeto no esté dirigida a un programa o dato en particular.

Por su parte, la sección 2 de la Ley está dedicada al acceso no autorizado con intención de cometer o facilitar la comisión de nuevos delitos, estableciendo las penas para el sujeto que lleve a cabo los

---

*(a)on summary conviction in England and Wales, to imprisonment for a term not exceeding 12 months or to a fine not exceeding the statutory maximum or to both;*
*(b)on summary conviction in Scotland, to imprisonment for a term not exceeding [F4 12] months or to a fine not exceeding the statutory maximum or to both;*
*(c)on conviction on indictment, to imprisonment for a term not exceeding two years or to a fine or to both.]*
*F1 Words in s. 1(1)(a) inserted (S.) (1.10.2007) by Police and Justice Act 2006 (c. 48), ss. 35(2)(a), 53 (with s. 38(1)); S.S.I. 2007/434, art. 2 (the inserting provision being repealed for E.W.N.I. (1.10.2008) by 2007 c. 27, ss. 61(2), 92, 94, Sch. 14 (with Sch. 13 para. 5); S.I. 2008/2504, art. 2(a)(i)(viii))*
*F2 Words in s. 1(1)(b) inserted (S.) (1.10.2007) by Police and Justice Act 2006 (c. 48), ss. 35(2)(b), 53 (with s. 38(1)); S.S.I. 2007/434, art. 2 (the inserting provision being repealed for E.W.N.I. (1.10.2008) by 2007 c. 27, ss. 61(2), 92, 94, Sch. 14 (with Sch. 13 para. 5); S.I. 2008/2504, art. 2(a)(i)(viii))*
*F3 S. 1(3) substituted (1.10.2007 for S. and 1.10.2008 otherwise) by Police and Justice Act 2006 (c. 48), ss. 35(3), 53 (with s. 38(2)(6)); S.S.I. 2007/434, art. 2; S.I. 2008/2503, art. 2(a)*
*F4 Word in s. 1(3)(b) substituted (3.5.2015) by Serious Crime Act 2015 (c. 9), s. 88(1), Sch. 4 para. 7(a); S.I. 2015/820, reg. 2(r)(iii)".*

delitos previstos en la sección 1 con la intención de cometer el delito a los que se refiere esta sección o para facilitar su comisión[223].

---

La sección 2 de la Ley, tras las reformas llevadas a cabo por la "*Police and Justice Act 2006*" y el "*Serious Crime Act 2015*", establece: "*Unauthorised access with intent to commit or facilitate commission of further offences.*

*(1)A person is guilty of an offence under this section if he commits an offence under section 1 above ("the unauthorised access offence") with intent—*

*(a)to commit an offence to which this section applies; or*

*(b)to facilitate the commission of such an offence (whether by himself or by any other person);and the offence he intends to commit or facilitate is referred to below in this section as the further offence.*

*(2)This section applies to offences—*

*(a)for which the sentence is fixed by law; or*

*(b)for which a person who has attained the age of twenty-one years (eighteen in relation to England and Wales) and has no previous convictions may be sentenced to imprisonment for a term of five years (or, in England and Wales, might be so sentenced but for the restrictions imposed by section 33 of the M1Magistrates' Courts Act 1980).*

*(3)It is immaterial for the purposes of this section whether the further offence is to be committed on the same occasion as the unauthorised access offence or on any future occasion.*

*(4)A person may be guilty of an offence under this section even though the facts are such that the commission of the further offence is impossible.*

*[F5(5)A person guilty of an offence under this section shall be liable—*

*(a)on summary conviction in England and Wales, to imprisonment for a term not exceeding 12 months or to a fine not exceeding the statutory maximum or to both;*

*(b)on summary conviction in Scotland, to imprisonment for a term not exceeding [F612] months or to a fine not exceeding the statutory maximum or to both;*

*(c)on conviction on indictment, to imprisonment for a term not exceeding five years or to a fine or to both.].*

*F5 S. 2(5) substituted (1.10.2007 for S. and 1.10.2008 otherwise) by Police and Justice Act 2006 (c. 48), ss. 52, 53, Sch. 14 para. 17 (with s. 38(6)); S.S.I.*

La citada norma también se ocupa en su sección 3[224] de regular

*2007/434, art. 2; S.I. 2008/2503, art. 2(c)*
*F6 Word in s. 2(5)(b) substituted (3.5.2015) by Serious Crime Act 2015 (c. 9), s. 88(1), Sch. 4 para. 7(b); S.I. 2015/820, reg. 2(r)(iii)".*

[224] Sección 3: *"[F73 Unauthorised acts with intent to impair, or with recklessness as to impairing, operation of computer, etc. (1) A person is guilty of an offence if—(a)he does any unauthorised act in relation to a computer;(b) at the time when he does the act he knows that it is unauthorised; and(c) either subsection (2) or subsection (3) below applies. (2)This subsection applies if the person intends by doing the act—(a) to impair the operation of any computer; (b) to prevent or hinder access to any program or data held in any computer; [F8or] (c) to impair the operation of any such program or the reliability of any such data; [F9or (d) to enable any of the things mentioned in paragraphs (a) to (c) above to be done.]] (3) This subsection applies if the person is reckless as to whether the act will do any of the things mentioned in paragraphs (a) [F10to (d)][F10to (c)] of subsection (2) above. (4) The intention referred to in subsection (2) above, or the recklessness referred to in subsection (3) above, need not relate to—(a) any particular computer; (b) any particular program or data; or (c) a program or data of any particular kind. (5) In this section—(a)a reference to doing an act includes a reference to causing an act to be done; (b)"act" includes a series of acts; (c)a reference to impairing, preventing or hindering something includes a reference to doing so temporarily. (6) A person guilty of an offence under this section shall be liable—(a)on summary conviction in England and Wales, to imprisonment for a term not exceeding 12 months or to a fine not exceeding the statutory maximum or to both;(b)on summary conviction in Scotland, to imprisonment for a term not exceeding [F1112] months or to a fine not exceeding the statutory maximum or to both; (c)on conviction on indictment, to imprisonment for a term not exceeding ten years or to a fine or to both.*

*Amendments (Textual)*

*F7 S. 3 substituted (1.10.2007 for S. and 1.10.2008 otherwise) by Police and Justice Act 2006 (c. 48), ss. 36, 53 (with s. 38(3)(4)(6)); S.S.I. 2007/434, art. 2; S.I. 2008/2503, art. 2 (the substituting provision being amended for E.W.N.I. (1.10.2008) by 2007 c. 27, ss. 61(3), 94 (with Sch. 13 para. 5); S.I. 2008/2504, art. 2(a))*
*F8 Word at the end of s. 3(2)(b) inserted (E.W.N.I.) (1.10.2008) by virtue of Serious Crime Act 2007 (c. 27), ss. 61(3)(a)(i), 94 (with Sch. 13 para. 5); S.I.*

cualquier otra conducta llevada a cabo con intención de perjudicar, o con imprudencia en cuanto al perjuicio, el funcionamiento del sistema informático, si el sujeto realiza el acto no autorizado en relación con ese sistema y sabe que no está autorizado. En concreto, en su apartado 2 se regulan esos delitos si el sujeto perjudica la operación de cualquier sistema, o impide o dificulta el acceso a cualquier programa o datos almacenados que contenga, o para perjudicar la operación de cualquier programa o la fiabilidad de tales datos, o para permitir cualquiera de las conductas mencionadas en este apartado 2. Su apartado 3 regula los supuestos en el que el sujeto es imprudente en los hechos del apartado 2. Por último, destaca de nuevo que su apartado 5 también se ocupe de interpretar algunos de los conceptos de la sección.

Por su parte, la sección 3A tipifica las conductas de hacer, suministrar u obtener artículos para la comisión de los citados delitos previstos en la sección 1 o 3, que tendría su equivalente en el artículo 197 *ter* del Código español, al que se dedica el Capítulo IV de este trabajo.

---

*2008/2504, art. 2(a)*
*F9 S. 3(2)(d) and preceding word repealed (E.W.N.I.) (1.10.2008) by virtue of Serious Crime Act 2007 (c. 27), ss. 61(3)(a)(ii), 92, 94, Sch. 14 (with Sch. 13 para. 5); S.I. 2008/2504, art. 2(a)(i)(viii)*
*F10 S. 3(3): Words "to (c)" substituted for words "to (d)" (E.W.N.I.) (1.10.2008) by virtue of Serious Crime Act 2007 (c. 27), ss. 61(3)(b), 94 (with Sch. 13 para. 5); S.I. 2008/2504, art. 2(a)*
*F11 Word in s. 3(6)(b) substituted (3.5.2015) by Serious Crime Act 2015 (c. 9), s. 88(1), Sch. 4 para. 7(c); S.I. 2015/820, reg. 2(r)(iii)".*

Además de las previsiones interpretativas dentro de algunos de los citados preceptos, la norma también dedica un precepto a la interpretación de la ley en general. En concreto, conforme a su sección 17[225] se entiende que una persona asegura el acceso a cualquier

[225] Sección 17: "*Interpretation. (1)The following provisions of this section apply for the interpretation of this Act. (2)A person secures access to any program or data held in a computer if by causing a computer to perform any function he—(a)alters or erases the program or data; (b)copies or moves it to any storage medium other than that in which it is held or to a different location in the storage medium in which it is held; (c)uses it; or (d)has it output from the computer in which it is held (whether by having it displayed or in any other manner);and references to access to a program or data (and to an intent to secure such access [F76or to enable such access to be secured]) shall be read accordingly. (3) For the purposes of subsection (2)(c) above a person uses a program if the function he causes the computer to perform—(a)causes the program to be executed; or (b)is itself a function of the program. (4) For the purposes of subsection (2)(d) above—(a)a program is output if the instructions of which it consists are output; and (b)the form in which any such instructions or any other data is output (and in particular whether or not it represents a form in which, in the case of instructions, they are capable of being executed or, in the case of data, it is capable of being processed by a computer) is immaterial. (5) Access of any kind by any person to any program or data held in a computer is unauthorised if—(a)he is not himself entitled to control access of the kind in question to the program or data; and (b)he does not have consent to access by him of the kind in question to the program or data from any person who is so entitled [F77but this subsection is subject to section 10.] (6) References to any program or data held in a computer include references to any program or data held in any removable storage medium which is for the time being in the computer; and a computer is to be regarded as containing any program or data held in any such medium.*
*(7)F78. . . . . .*
*[F79(8)An act done in relation to a computer is unauthorised if the person doing the act (or causing it to be done)—(a)is not himself a person who has responsibility for the computer and is entitled to determine whether the act may be done; and (b)does not have consent to the act from any such*

programa o datos almacenados en un sistema informático si provoca que realice cualquier función de alterar o borrar el programa o los datos, copiar o moverlos a otra ubicación, utilizarlos o darles salida desde el sistema. Se considera a estos efectos que una persona utiliza un programa si la función que provoca en el sistema hace que el programa sea ejecutado o esa función es en sí misma una función del programa.

En cuanto al acceso a un programa o datos contenidos en un sistema informático se considera no autorizado si el sujeto no tiene derecho a controlar el programa o datos y no tiene consentimiento de la persona con derecho para el acceso.

Además, se considera que la referencia a cualquier programa o datos contenidos en un sistema informático comprende cualquier

---

*person. In this subsection " act " includes a series of acts. ]*
*(9)References to the home country concerned shall be read in accordance with section 4(6) above. (10)References to a program include references to part of a program.*
*F76 Words in s. 17(2) inserted (S.) (1.10.2007) by Police and Justice Act 2006 (c. 48), ss. 52, 53, Sch. 14 para. 29(2) (with s. 38(1)); S.S.I. 2007/434, art. 2 (the inserting provision being repealed for E.W.N.I. (1.10.2008) by 2007 c. 27, ss. 61(5), 92, 94, Sch. 14 (with Sch. 13 para. 5); S.I. 2008/2504, art. 2(a)(i)(viii))*
*F77 Words in s. 17(5)(b) inserted (3.2.1995) by 1994 c. 33, s. 162(2); S.I. 1995/127, art. 2(1), Sch. 1*
*F78 S. 17(7) repealed (1.10.2007 for S. and 1.10.2008 otherwise) by Police and Justice Act 2006 (c. 48), ss. 52, 53, Sch. 14 para. 29(3), Sch. 15 Pt. 4 (with s. 38(4)); S.S.I. 2007/434, art. 2; S.I. 2008/2503, art. 2*
*F79 S. 17(8) substituted (1.10.2007 for S. and 1.10.2008 otherwise) by Police and Justice Act 2006 (c. 48), ss. 52, 53, Sch. 14 para. 29(4) (with s. 38(4)); S.S.I. 2007/434, art. 2; S.I. 2008/2503, art. 2.".*

programa o datos almacenados en un medio de almacenamiento extraíble, y un sistema informático se considera el que contiene cualquier programa o datos contenidos en este medio.

Por último, la sección 17 también se ocupa de interpretar las conductas no autorizadas llevadas a cabo en un sistema informático, considerando que el sujeto que responde penalmente no es la misma persona que tiene responsabilidad sobre el sistema y derecho a determinar los actos que pueden realizarse y además no tiene el consentimiento de esta persona.

Por tanto, en el caso de Reino Unido, es destacable que el legislador haya optado por tipificar los delitos informáticos en una ley penal especial, y además, al igual que el legislador portugués, lo haya realizado con una regulación extensa y minuciosa que es anterior incluso a los instrumentos y directivas europeas.

### *3. PAÍSES QUE REGULAN EL DELITO DE HACKING EN UN TÍTULO O CAPÍTULO PROPIO Y DIFERENCIADO.*

Se incluye en este epígrafe una breve aproximación a las legislaciones de los países europeos que han optado por dotar de cierta autonomía a los delitos de *hacking*.

Sin llegar hasta el punto de tipificar estos delitos en la legislación penal especial como en los casos mencionados en el epígrafe anterior, se regula el intrusismo informático en un título,

capítulo o sección propia del Código penal, de forma independiente a otros delitos. Así pues, en este apartado se citan los supuestos de Bélgica, Bulgaria, Croacia, Finlandia y Hungria, que se exponen brevemente, con referencia igualmente a sus peculiaridades en relación con la regulación española, a la que se dedicarán los Capítulos siguientes.

### *3.1 Bélgica.*

En el ámbito belga, el Código penal de 8 de junio de 1867[226] dedica el Título IX *bis* a los delitos contra la confidencialidad, integridad y disponibilidad de los sistemas y datos informáticos almacenados, procesados o transmitidos por estos sistemas, introducido por la Ley 2000-11-28-/34. Dentro de este título, el artículo 550 *bis* regula en su primer apartado las conductas de acceso al sistema informático o mantenimiento dentro del mismo a sabiendas de que no está permitido, incrementando las penas en el mismo apartado para el que lleve a cabo las conductas con una intención fraudulenta. Por tanto, el tipo del delito de *hacking* no exige la

[226] Código penal disponible en http://www.ejustice.just.fgov.be/cgi_loi/loi_a1.pl?DETAIL=1867060801%2FF&caller=list&row_id=1&numero=2&rech=4&cn=1867060801&table_name=LOI&nm=1867060850&la=F&dt=CODE+PENAL&language=fr&fr=f&choix1=ET&choix2=ET&fromtab=loi_all&trier=promulgation&chercher=t&sql=dt+contains++%27CODE%27%26+%27PENAL%27and+actif+%3D+%27Y%27&tri=dd+AS+RANK+&imgcn.x=41&imgcn.y=12#LNK0117, consultado el 12 de enero de 2017.

vulneración de medidas de seguridad en el acceso al sistema de información, que facultaba para incluir el artículo 2 de la DM 2005/222/JAI y viene impuesta en el artículo 3 de la Directiva 2013/40/UE. Además, de forma similar al artículo 197 *bis* 1 del Código Penal español, el tipo básico no viene referido al acceso a datos o programas, sino al sistema informático, incluyendo el tipo de mantenimiento no autorizado en el sistema.

El apartado segundo establece una agravante para el que con intención de defraudar o dañar se exceda en sus facultades de acceso a un sistema informático y el apartado tercero castiga con mayores penas al sujeto cuando en las conductas citadas en los apartados 1 y 2 sean recogidos los datos almacenados, procesados o transmitidos por el sistema informático, sea utilizado éste para acceder al de un tercero o se cause algún daño al sistema o a los datos que almacene, procese o transmita. La tentativa para la comisión de los tipos básicos de los apartados 1 y 2 se castiga con sus mismas penas en el apartado 4, incluyéndose por tanto expresamente estos supuestos dentro del mismo precepto, a diferencia del Código español, que regula la tentativa en su parte general, artículo 16, con las consecuencias del artículo 62.

En el apartado 5 se tipifican los hechos en los que se posea, produzca, venda o ponga a disposición de otras personas dispositivos o datos informáticos para cometer los anteriores delitos, de forma similar a como se regulan estas conductas en el artículo 197 *ter* del Código español tras la reforma de la LO 1/2015.

Como agravante común a los apartados 1 a 5, se establece en su apartado 6 la consistente en ordenar o incitar la comisión de alguna de las conductas citadas, regulando en el apartado 7 la revelación de los datos en los delitos regulados en los tres primeros apartados y duplicando el apartado 8 cada una de las penas previstas en este artículo en los casos de reincidencia en un plazo de cinco años[227],

[227] Artículo 550 *bis*: *"<inséré par L 2000-11-28/34, art. 6; En vigueur : 13-02-2001> § 1er. Celui qui, sachant qu'il n'y est pas autorisé, accède à un système informatique ou s'y maintient, est puni d'un emprisonnement de trois mois à un an et d'une amende de vingt-six [euros] à vingt-cinq mille [euros] ou d'une de ces peines seulement. <L 2000-06-26/42, art. 2, En vigueur : 01-01-2002> Si l'infraction visée à l'alinéa 1er, est commise avec une intention frauduleuse, la peine d'emprisonnement est de six mois à deux ans. § 2. Celui qui, avec une intention frauduleuse ou dans le but de nuire, outrepasse son pouvoir d'accès à un système informatique, est puni d'un emprisonnement de six mois à deux ans et d'une amende de vingt-six [euros] à vingt-cinq mille [euros] ou d une de ces peines seulement. <L 2000-06-26/42, art. 2, En vigueur : 01-01-2002> § 3. Celui qui se trouve dans une des situations visées aux §§ 1er et 2 et qui : 1° soit reprend, de quelque manière que ce soit, les données stockées, traitées ou transmises par le système informatique; 2° soit fait un usage quelconque d'un système informatique appartenant à un tiers ou se sert du système informatique pour accéder au système informatique d'un tiers; 3° soit cause un dommage quelconque, même non intentionnellement, au système informatique ou aux données qui sont stockées traitées ou transmises par ce système ou au système informatique d'un tiers ou aux données qui sont stockées, traitées ou transmises par ce système; est puni d'un emprisonnement de un à trois ans et d'une amende de vingt-six [euros] belges à cinquante mille [euros] ou d'une de ces peines seulement. <L 2000-06-26/42, art. 2, En vigueur : 01-01-2002> § 4. La tentative de commettre une des infractions visées aux §§ 1er et 2 est punie des mêmes peines. § 5. (Celui qui, indûment, possède, produit, vend, obtient en vue de son utilisation, importe, diffuse ou met à disposition sous une autre forme, un quelconque dispositif, y compris des données informatiques, principalement conçu ou adapté pour permettre la commission des infractions prévues au §§ 1er à 4, est puni d'un*

estando por tanto prevista en este mismo precepto, a diferencia del Código español que la regula en su parte general, artículo 22.8º.

De forma paralela con el precepto anterior, su artículo 550 *ter*[228] regula los delitos cometidos por el que a sabiendas de no estar

---

*emprisonnement de six mois à trois ans et d'une amende de vingt-six euros à cent mille euros ou d'une de ces peines seulement.) <L 2006-05-15/46, art. 5, 059; En vigueur : 22-09-2006> § 6. Celui qui ordonne la commission d'une des infractions visées aux §§ 1er à 5 ou qui y incite, est puni d'un emprisonnement de six mois à cinq ans et d'une amende de cent [euros] à deux cent mille [euros] ou d'une de ces peines seulement. <L2000-06-26/42, art. 2, En vigueur : 01-01-2002> § 7. Celui qui, sachant que des données ont été obtenues par la commission d'une des infractions visées aux §§ 1er à 3, les détient, les révèle à une autre personne ou les divulgue, ou fait un usage quelconque des données ainsi obtenues, est puni d'un emprisonnement de six mois à trois ans et d'une amende de vingt-six [euros] à cent mille [euros] ou d'une de ces peines seulement. <L 2000-06-26/42, art. 2, En vigueur : 01-01-2002> § 8. Les peines prévues par les §§ 1er à 7 sont doublées si une infraction à l'une de ces dispositions est commise dans les cinq ans qui suivent le prononcé d'une condamnation pour une de ces infractions ou pour une des infractions visées aux articles 210bis, 259bis, 314bis, 504quater ou 550ter.*".

[228] Artículo 550 *ter*: *"<inséré par L 2000-11-28/34, art. 6; ED : 13-02-2001> § 1er. (Celui qui, sachant qu'il n'y est pas autorisé, directement ou indirectement, introduit dans un système informatique, modifie ou efface des données, ou qui modifie par tout moyen technologique l'utilisation normale de données dans un système informatique, est puni d'un emprisonnement de six mois à trois ans et d'une amende de vingt-six euros à vingt-cinq mille euros ou d'une de ces peines seulement. Si l'infraction visée à l'alinéa 1er est commise avec une intention frauduleuse ou dans le but de nuire, la peine d'emprisonnement est de six mois à cinq ans.) <L 2006-05-15/46, art. 6, 1°, 059; En vigueur : 22-09-2006> § 2. Celui qui, suite à la commission d'une infraction visée au § 1er, cause un dommage à des données dans le système informatique concerné ou dans tout autre système informatique, est puni d'un emprisonnement de six mois à cinq ans et d'une amende de vingt-six [euros] à septante-cinq mille [euros] ou d'une de ces*

autorizado, directa o indirectamente, se introduce en un sistema informático, modifica o borra los datos, o altera por cualquier medio tecnológico la normal utilización de los datos en un sistema informático, incrementando las penas en el mismo apartado 1 en el caso de que se haya cometido con intención fraudulenta o con ánimo de causar daños, y estableciendo mayor castigo en su apartado 2 si se llegan a causar los daños.

Finalmente, las penas son superiores en su apartado 3 cuando en los supuestos del apartado 1 se llega a impedir total o parcialmente el correcto funcionamiento del sistema informático, así como en el apartado 4 para los casos en que, en relación con los delitos de los tres

---

*peines seulement. <L 2000-06-26/42, art. 2, En vigueur : 01-01-2002> § 3. Celui qui, suite à la commission d'une infraction visée au § 1er, empêche, totalement ou partiellement, le fonctionnement correct du système informatique concerné ou de tout autre système informatique, est puni d'un emprisonnement de un an à cinq ans et d'une amende de vingt-six [euros] à cent mille [euros] ou d'une de ces peines seulement. <L 2000-06-26/42, art. 2, En vigueur : 01-01-2002> § 4. (Celui qui, indûment, possède, produit, vend, obtient en vue de son utilisation, importe, diffuse ou met à disposition sous une autre forme, un dispositif y compris des données informatiques, principalement conçu ou adapté pour permettre la commission des infractions prévues au §§ 1er à 3, alors qu'il sait que ces données peuvent être utilisées pour causer un dommage à des données ou empêcher, totalement ou partiellement, le fonctionnement correct d'un système informatique, euros à cent mille euros ou d'une de ces peines seulement.) <L 2006-05-15/46, art. 6, 2°, 059; En vigueur : 22-09-2006> § 5. Les peines prévues par les §§ 1er à 4 sont doublées si une infraction à l'une de ces dispositions est commise dans les cinq ans qui suivent le prononcé d'une condamnation pour une de ces infractions ou pour une des infractions visées aux articles 210bis, 259bis, 314bis, 504quater ou 550bis. (§ 6. La tentative de commettre l'infraction visée au § 1er est punie des mêmes peines.) <L 2006-05-15/46, art. 6, 3°, 059; En vigueur : 22-09-2006>*".

primeros apartados, indebidamente se posee, produce, vende, importa, distribuye o pone a disposición de otra persona datos o dispositivos para llevar a cabo esas conductas, duplicando el apartado 5 las penas en los supuestos de reincidencia en los delitos de los apartados 1 a 4 dentro del plazo de cinco años y concluyendo en su apartado 6 con la regulación de la tentativa para cometer el delito de su primer apartado, que conlleva la misma pena.

Por tanto, en el Código belga destaca la tipificación de los delitos contra los sistemas informáticos en un título propio, más acorde con las exigencias de la realidad tecnológica y separado de otros delitos que tutelan bienes jurídicos distintos, tal y como se expondrá en el siguiente Capítulo. Además, en los mismos preceptos donde regula el intrusismo informático se incluye la citada agravante de reincidencia y la tentativa, facilitando así la interpretación de estos supuestos al no tener que recurrir a la parte general del Código para relacionarla con estas conductas, que en otro caso tendrían su regulación en sus artículos 51 y 52 dedicados a la tentativa, o en sus artículos 54 a 57 *bis* en los supuestos de reincidencia.

### *3.2 Bulgaria.*

Tras la reforma del año 2007 del Código penal búlgaro[229], su

[229] La versión en inglés del Código penal búlgaro, incluyendo la reforma introducida en el año 2002 por la SG 92/02, se encuentra en

artículo 93 contiene la definición de sistema informático, relativo al dispositivo individual o conjunto de dispositivos interconectados o similares que, en cumplimiento de un programa definido, proporciona un procesamiento automático de datos. Se toman así las pautas que proporciona la definición del artículo 2.a) de la Directiva 2013/40/UE, aunque sin incluir dentro del concepto también los datos almacenados, tratados, recuperados o transmitidos por dicho aparato o grupo de aparatos para su funcionamiento, utilización, protección y mantenimiento. El mismo artículo 93 incluye el concepto de datos informáticos, que se relacionan con la presentación de hechos, información o conceptos sujetos a un tratamiento automatizado[230].

En concreto, las conductas de *hacking* se encuentran reguladas en el artículo 319a[231], de su capítulo nueve, bajo la rúbrica relativa al

---

http://www.legislationline.org/documents/action/popup/id/8881/preview, consultado el 12 de enero de 2017.

[230] Artículo 93: "*21. (New, SG No. 92/2002, amended, SG No. 38/2007) A "computerized system" is any device or a group of interconnected or related devices, one or more of which, pursuant to a program, performs automatic processing of data.*
*22. (New, SG No. 92/2002, amended, SG No. 38/2007) "Computerized data" is any representation of facts, information or concepts in a form suitable for automatic processing, including computer programs* ".

[231] Artículo 319a. "*((1) (Amended, SG No. 38/2007) Anyone who copies, uses or obtains access to computer data in a computer system without permission, where such is required, shall be punished by a fine of up to BGN three thousand.*

*(2) Where the act under par. 1 has been committed by two or more people, who have previously agreed so to do, the punishment shall be deprivation of liberty of up to one year or a fine of up to BGN three thousand.*

cibercrimen, castigando a quien copie, use u obtenga el acceso no autorizado a datos contenidos en un sistema informático. Por tanto, a diferencia del Código español, el tipo de *hacking* en el Código búlgaro no exige la vulneración de medidas de seguridad que impone el artículo 3 de la Directiva 2013/40/UE y tampoco contempla los supuestos de mantenimiento no autorizado en el sistema informático.

El mismo artículo 319a establece en su apartado segundo mayores penas si la conducta se ha cometido por dos o más personas de común acuerdo previo y regula en su apartado tercero los supuestos de reincidencia en relación con estas conductas, a diferencia del Código español que la regula como agravante genérica en su parte general. En los supuestos que cualquiera de las acciones de los apartados 1 a 3 afecten a secretos de Estado se prevén mayores penas.

Por último, el apartado 5 castiga los casos de consecuencias graves por la comisión del delito del apartado 4.

En consecuencia, el legislador búlgaro ha optado por aportar

---

*(3) (Amended, SG No. 38/2007) Where the act under par. 1 is repeated or is with regard to data for creation of an electronic signature, the punishment shall be deprivation of liberty of up three years or a fine of up to BGN five thousand.*

*(4) (Amended, SG No. 26/2004, supplemented, SG No. 38/2007) Where acts under paragraphs 1-3 have been committed with regard to information that qualifies as a secret of the State or to another information protected by the law, the punishment shall be deprivation of liberty from one to three years, unless severer punishment has been envisaged.*

*(5) Where grave consequences have occurred as a result of the acts under par. 4, punishment shall be of one to eight years"*.

claridad en la regulación de estos delitos, estableciendo un precepto para definiciones y dedicando un capítulo específico al cibercrimen, a diferencia del legislador español, que tanto con la reforma de 2010 como con la reforma de 2015 ha incluido el acceso ilícito a los sistemas informáticos entre los delitos contra la intimidad con los consiguientes problemas interpretativos en torno al bien jurídico protegido, que serán expuestos en el Capítulo III de este trabajo.

### *3.3 Croacia.*

En el ámbito croata, tras la reforma de 15 de julio de 2003[232],

[232] La reforma del Código penal por la Ley de 15 de julio de 2003 disponible en http://narodne-novine.nn.hr/clanci/sluzbeni/2003_07_111_1496.html, consultado el 12 de enero de 2017, incluyendo el *hacking* en su artículo 223: "*Naziv članka 223. mijenja se i glasi: »Povreda tajnosti, cjelovitosti i dostupnosti računalnih podataka, programa ili sustava«.*

*Članak 223. mijenja se i glasi: »(1) Tko unatoč zaštitnim mjerama neovlašteno pristupi računalnim podacima ili programima, kaznit će se novčanom kaznom ili kaznom zatvora do tri godine.*

*(2) Tko onemogući ili oteža rad ili korištenje računalnih sustava, računalnih podataka ili programa ili računalnu komunikaciju, kaznit će se novčanom kaznom ili kaznom zatvora do tri godine.*

*(3) Tko ošteti, izmijeni, izbriše, uništi ili na drugi način učini neuporabljivim ili nedostupnim tuđe računalne podatke ili raču-nalne programe, kaznit će se novčanom kaznom ili kaznom zatvora do tri godine.*

*(4) Tko presreće ili snimi nejavni prijenos računalnih podatka koji mu nisu namijenjeni prema, unutar ili iz računalnog sustava, uključujući i elektromagnetske emisije računalnog sustava koji prenosi te podatke, ili tko omogući nepozvanoj osobi da se upozna s takvim podacima, kaznit će se novčanom kaznom ili kaznom zatvora do tri godine.*

*(5) Ako je kazneno djelo iz stavka 1., 2., 3. ili 4. ovoga članka počinjeno u odnosu na računalni sustav, podatak ili program tijela državne vlasti, javne ustanove ili trgovačkog društva od posebnoga javnog interesa, ili je prouzročena znatna šteta, počinitelj će se kazniti kaznom zatvora od tri mjeseca do pet godina.*

*(6) Tko neovlašteno izrađuje, nabavlja, prodaje, posjeduje ili čini drugome dostupne posebne naprave, sredstva, računalne programe ili računalne podatke stvorene ili prilagođene za činjenje kaznenog djela iz stavka 1., 2., 3. ili 4. ovoga članka,*

*kaznit će se novčanom kaznom ili kaznom zatvora do tri godine.*

*(7) Posebne naprave, sredstva, računalni programi ili podaci stvoreni, korišteni ili prilagođeni za činjenje kaznenih djela, a kojima je počinjeno kazneno djelo iz stavka 1., 2., 3. ili 4. ovoga članka oduzet će se.*

*(8) Za pokušaj kaznenog djela iz stavka 1., 2., 3. ili 4. ovoga članka počinitelj će se kazniti".*

En su versión inglesa: "*(1) Whoever, without authorization despite the protective measures, accesses the computer data or programs of another shall be punished by a fine or by imprisonment not exceeding three years. (2) Whoever renders unusable or hinders the work or the use of computer systems, computer programs or electronic data and communication shall be punished by a fine or by imprisonment not exceeding three years. (3) Whoever damages, alters, deletes, destroys or in some other way renders unusable or inaccessible the electronic data or computer programs of another shall be punished by a fine or by imprisonment not exceeding three years. ( 4) Whoever intercepts or records the nonpublic transmission of electr onic data to, within or from a computer system, not intended for hi s use, including the electromagnetic transmissions of data in the computer s ystem, or whoever enables an unauthorized person to access these data shall be punished by a fine or by imprisonment not exceeding thr ee years. (5) If the ccriminal offense referred to in paragraph s 1 , 2, 3 and 4 of this Article is committed in connection with the computer system, electronic data or co mputer program of a governmental body, a public institution or a company of special public interest, or if significant damage is caused, the perpetrator sh all be punished by imprisonment for three months to five years. (6) Whoev er, without uthorization, produces, procures, sells, possesses or makes avail*

los delitos de *hacking* se encontraban regulados en el artículo 223 de su Código penal de 1997[233], relativo a los daños a datos y uso de datos ajenos, dentro del Capítulo XVII, que estaba dedicado a los delitos contra la propiedad.

El tipo básico castigaba al que sin autorización y a pesar de las medidas de seguridad accedía a los datos o programas informáticos ajenos, y el mismo precepto se ocupaba de las conductas relativas a inutilizar o dificultar el uso de sistemas informáticos o datos electrónicos y comunicaciones (apartado 2), dañar, alterar, borrar, destruir, inutilizar o hacer inaccesibles datos electrónicos o programas informáticos ajenos (apartado 3), interceptar o grabar la transmisión de datos no públicos dentro o desde un sistema informático o permitir este acceso a persona no autorizada (apartado 4), incrementando las penas en todos estos casos cuando los delitos cometidos guardaran relación con el sistema informático, datos electrónicos o programas

---

*able o another person special devices, equipment, computer programs and electronic data created or adapted for the perpetration of the criminal offe nse referred to in paragraphs 1, 2, 3 and 4 of this Article shall be punished by a fine or by imprisonment not exceeding three years. (7) Special devices , equipment, computer programs or electronic data created, used or adapte d for the perpetration of criminal offenses and used fot the perpetration of t he criminal offense referred to in paragraphs 1, 2, 3 and 4 of this Article sha ll be forfeited. (8) Whoever attempts to perpetrate the criminal offenses ref erred to in paragraphs 1, 2, 3 and 4 of this Article shall be punished".*

[233] Código penal de 21 de octubre de 1997 disponible en http://narodne-novine.nn.hr/clanci/sluzbeni/1997_10_110_1668.html. Versión inglesa en http://www.legislationline.org/documents/section/criminal-codes, consultado el 12 de enero de 2017.

informáticos gubernamentales o de una institución pública o una empresa de especial interés público, o bien los daños son significativos (apartado 5).

Por último, en relación con las conductas de los apartados 1 a 4, se establecían las penas para el que sin autorización producía, procuraba, vendía, poseía o ponía a disposición de otra persona dispositivos especiales, equipos, programas informáticos y datos electrónicos creados o adaptados para cometer esos delitos (apartado 6), que serían decomisados (apartado 7), contemplando también en el último apartado la tentativa para la comisión de los delitos.

En el nuevo Código penal croata[234], el capítulo XXV está dedicado a los delitos contra los sistemas informáticos, programas y datos, regulándose por tanto en una categoría propia, siguiendo un criterio distinto al del legislador español. El acceso no autorizado se tipifica en el artículo 266, cuyo primer apartado regula el acceso no autorizado a datos o sistemas informáticos, incrementando la pena el segundo apartado en el caso de sistemas o cuerpos de datos informatizados del Estado u organismos o empresas públicas, incluyendo la tipificación de la tentativa[235]. La referencia es por tanto

[234] El nuevo Código penal de 26 de octubre de 2011 está disponible en http://narodne-novine.nn.hr/clanci/sluzbeni/2011_11_125_2498.html, consultado el 12 de enero de 2017.

[235] El artículo 266 establece: "*GLAVA DVADESET PETA (XXV.) KAZNENA DJELA PROTIV RAČUNALNIH SUSTAVA, PROGRAMA I PODATAKA Neovlašteni pristup Članak 266. (1) Tko neovlašteno pristupi računalnom sustavu ili računalnim podacima, kaznit će se kaznom zatvora do jedne godine. (2) Tko kazneno djelo iz stavka 1. ovoga članka počini u odnosu na*

a datos, como los incluidos en el anterior artículo 197.3 del Código español, o sistemas informáticos, más ajustado al actual artículo 197 *bis* 1 tras la reforma de la LO 1/2015, relativo a sistemas de información.

A diferencia del Código español, el capítulo no contiene referencia a las conductas de permanencia en el sistema, ni tampoco menciona la vulneración de medidas de seguridad en el acceso al sistema informático que exige el artículo 3 de la Directiva 2013/40/UE. Sin embargo, incluye la obstrucción del sistema informático (artículo 267); los daños informáticos (artículo 268); la interceptación de datos informáticos (artículo 269); falsificación informática (artículo 270); el acceso ilícito, alteración, borrado, daño o hacer inutilizable o inaccesible los datos informáticos con ánimo de lucro propio o ajeno, con penas incrementadas si hay un beneficio sustancial o daño considerable (artículo 271), circunstancia que contemplaba el anterior artículo 197.7 del Código español y que tras la reforma de la LO 1/2015 ya no resulta aplicable al *hacking*.

Por último, se regulan en el artículo 272 los supuestos de crear, suministrar, vender, poseer, poner a disposición de otros dispositivos o equipos o datos electrónicos creados o adaptados para la comisión de

---

*raĉunalni sustav ili raĉunalne podatke tijela drţavne vlasti, tijela jedinica lokalne ili područne (regionalne) samouprave, javne ustanove ili trgovaĉkog društva od posebnog javnog interesa, kaznit će se kaznom zatvora do tri godine. (3) Za pokušaj kaznenog djela iz stavka 1. i 2. ovoga ĉlanka poĉinitelj će se kazniti. (4) Kazneno djelo iz stavka 1. ovoga ĉlanka progoni se po prijedlogu.".*

los citados delitos, estableciendo su apartado segundo menores penas para el que crea, suministra, vende, posee o pone a disposición de otros contraseñas informáticas, códigos de acceso u otros datos con los que pueda accederse a un sistema informático con el objetivo de cometer algún delito de los previstos en los anteriores artículos[236], tipo similar al previsto en el actual artículo 197 *ter* del Código español.

Por tanto, en el Código croata de 1997 el *hacking* y los delitos que se regulaban en torno a estas conductas se consideraban desde el punto de vista de los atentados contra la propiedad, pero con el nuevo Código de 2011 se dedica un capítulo específico a delitos informáticos, donde tienen cabida tanto el acceso, como los daños, interceptaciones o la falsificación informática, lo que supone una nueva categoría de delitos más acorde con la revolución tecnológica acelerada que estamos experimentado y que exigiría en nuestro ámbito una ordenada actualización del Código Penal español o una nueva ley

---

236 El artículo 272 dispone: "*Zlouporaba naprava Ĉlanak 272. (1) Tko izradi, nabavi, proda, posjeduje ili ĉini drugome dostupne ureĆaje ili raĉunalne programe ili raĉunalne podatke stvorene ili prilagoĆene za poĉinjenje kaznenih djela iz ĉlanka 266., ĉlanka 267., ĉlanka 268., ĉlanka 269., ĉlanka 270. i ĉlanka 271. ovoga Zakona s ciljem da ih se uporabi za poĉinjenje nekog od tih djela, kaznit će se kaznom zatvora do tri godine. (2) Tko izradi, nabavi, proda, posjeduje ili ĉini drugome dostupne raĉunalne lozinke, pristupne šifre ili druge podatke kojima se moţe pristupiti raĉunalnom sustavu s ciljem da ih se uporabi za poĉinjenje kaznenih djela iz ĉlanka 266., ĉlanka 267., ĉlanka 268., ĉlanka 269., ĉlanka 270. i ĉlanka 271. ovoga Zakona, kaznit će se kaznom zatvora do jedne godine. (3) Poĉinitelj kaznenog djela iz stavka 1. ovoga ĉlanka neće se kazniti kaznom stroţom od one koja je propisana za kazneno djelo koje je imao za cilj. (4) Posebne naprave i programi iz stavka 1. ovoga ĉlanka će se oduzeti, a podaci iz stavka 1. i 2. ovoga ĉlanka će se uništiti*".

penal especial en la materia a efectos de lograr una ordenación lógica y coherente de los delitos en torno a la informática que se contienen de forma dispersa en el Código español.

### *3.4 Finlandia.*

En Finlandia el delito de *hacking* tiene su regulación penal en la sección 8, bajo la rúbrica de acceso informático, del capítulo 38 dedicado a los delitos contra la información y comunicaciones, de su Código penal de 1889[237], capítulo introducido por Ley 578/1995, de 21 de abril de 1995.

La citada sección fue reformada por la Ley 368/2015, de 10 de abril, y castiga al que mediante un código de acceso que no le pertenezca o por otro medio, quebrantando las medidas de seguridad ilegalmente acceda a un sistema informático, de forma similar a la impuesta por el artículo 3 de la Directiva 2013/40/UE, donde los datos son procesados, almacenados o transmitidos electrónicamente o de manera técnica similar, imponiendo iguales penas a la persona que sin acceder dentro del sistema o parte del mismo mediante un dispositivo técnico ilegalmente obtenga información contenida en el sistema informático. El precepto concluye regulando la tentativa y salvando

[237] Código Penal de 19 de diciembre de 1889 disponible en http://www.finlex.fi/fi/laki/ajantasa/1889/18890039001, consultado el 12 de enero de 2017.

estas conductas sólo para los casos en que el delito cometido no sea otro que conlleve pena igual o superior[238], lo que supone la tipificación expresa del criterio de alternatividad en la parte especial, que en el Código español tiene su previsión genérica dentro de su parte general, en el artículo 8.4[239].

La Sección 8 (a) establece como agravantes, tras la reforma por Ley 540/2007, el acceso llevado a cabo como parte de un grupo criminal organizado o si el acceso se produce de forma

---

238 La Sección 8, tras la Ley 368/2015, de 10 de abril, establece: "*8 § Tietomurto*
*Joka käyttämällä hänelle kuulumatonta käyttäjätunnusta taikka turvajärjestelyn muuten murtamalla oikeudettomasti tunkeutuu tietojärjestelmään, jossa sähköisesti tai muulla vastaavalla teknisellä keinolla käsitellään, varastoidaan tai siirretään tietoja tai dataa, taikka sellaisen järjestelmän erikseen suojattuun osaan, on tuomittava tietomurrosta sakkoon tai vankeuteen enintään kahdeksi vuodeksi.*
*Tietomurrosta tuomitaan myös se, joka tietojärjestelmään tai sen osaan tunkeutumatta*
*1) teknisen erikoislaitteen avulla tai*
*2) muuten teknisin keinoin turvajärjestelyn ohittaen, tietojärjestelmän haavoittuvuutta hyväksi käyttäen tai muuten ilmeisen vilpillisin keinoin oikeudettomasti ottaa selon 1 momentissa tarkoitetussa tietojärjestelmässä olevasta tiedosta tai datasta.*
*Yritys on rangaistava.*
*Tätä pykälää sovelletaan ainoastaan tekoon, josta ei ole muualla laissa säädetty ankarampaa tai yhtä ankaraa rangaistusta".*

239 En este sentido, el citado artículo 8.4 CP establece: "*Los hechos susceptibles de ser calificados con arreglo a dos o más preceptos de este Código, y no comprendidos en los artículos 73 a 77, se castigarán observando las siguientes reglas: (…) 4.ª En defecto de los criterios anteriores, el precepto penal más grave excluirá los que castiguen el hecho con pena menor*".

particularmente metódica[240], que tendría una regulación similar en el artículo 197 *quater* del Código español.

Por su parte, la Sección 8 (b)[241] regula los ataques basados en un dispositivo ilícito para el acceso a servicios protegidos, fijando las penas para el que ilegalmente, con fines comerciales o cuando el acto conduzca a causar un considerable perjuicio al proveedor de servicios protegidos, produzca, importe, ofrezca para la venta, alquile, o distribuya dispositivos ilícitos para acceder a servicios protegidos, o anuncie, instale o mantenga los mismos, a no ser que el hecho esté castigado con una pena igual o superior en otro precepto, atribuyendo carácter subsidiario a este delito, con una regulación similar a la del artículo 197 *ter* del Código español, si bien referidas a la actuación ilegal en el caso finlandés, en lugar de carecer de la debida

---

[240] La Sección 8 (a) dispone: "*8 a § Törkeä tietomurto*
*Jos tietomurto tehdään*
*1) osana 6 luvun 5 §:n 2 momentissa tarkoitetun järjestäytyneen rikollisryhmän toimintaa tai (8.5.2015/564)*
*2) erityisen suunnitelmallisesti ja tietomurto on myös kokonaisuutena arvostellen törkeä, rikoksentekijä on tuomittava törkeästä tietomurrosta sakkoon tai vankeuteen enintään kolmeksi vuodeksi.*
*Yritys on rangaistava*".

[241] La sección 8 (b) establece tras la Ley 919/2014, de 7 de noviembre de 2014, "*8 b § Suojauksen purkujärjestelmärikos.*
*Joka tietoyhteiskuntakaaren (917/2014) 269 §:n 2 momentissa säädetyn kiellon vastaisesti ansiotarkoituksessa tai siten, että teko on omiaan aiheuttamaan huomattavaa haittaa tai vahinkoa suojatun palvelun tarjoajalle, valmistaa, tuo maahan, pitää kaupan, vuokraa tai levittää suojauksen purkujärjestelmää, mainostaa sitä taikka asentaa tai huoltaa sitä, on tuomittava, jollei teosta muualla laissa säädetä ankarampaa tai yhtä ankaraa rangaistusta, suojauksen purkujärjestelmärikoksestasakkoon tai vankeuteen enintään yhdeksi vuodeksi".*

autorización, falta de autorización que por otra parte es el elemento exigido en el artículo 3 de la Directiva 2013/40/UE.

Por último, en relación con estas conductas, la Sección 11[242] establece el decomiso de los dispositivos ilícitos para el acceso a los servicios protegidos indicados en la Sección 8 (a).

Por tanto, destaca el establecimiento de una sección propia para el delito de acceso informático y un capítulo dedicado específicamente a los delitos contra la información y comunicaciones que, a diferencia de los Códigos que optan por incluirlos en el mismo capítulo que otros delitos que protegen bienes jurídicos distintos, es más acorde con la realidad tecnológica actual. Además, esta estructura sistemática finlandesa fue introducida tras reforma del año 1995, lo que evidencia la visión del legislador finlandés a la revolución acelerada que en materia de las nuevas tecnologías iba a suceder en los años siguientes.

Por otra parte, el tipo básico se refiere al acceso al sistema informático, de forma similar al artículo 197 *bis* 1 del Código español, pero destaca su amplitud y mayor protección de los bienes jurídicos implicados al comprender las conductas de conseguir la información contenida en el sistema. Esto conlleva también el acceso a datos o programas informáticos que preveía el anterior artículo 197.3 del

[242] Tras la Ley 368/2015, de 10 de abril de 2015, la sección 11 dispone: "*11 § Menettämisseuraamus.*
*Edellä 8 b §:ssä tarkoitettu suojauksen purkujärjestelmä on tuomittava valtiolle menetetyksi*.".

Código español con la reforma de la LO 5/2010, y que se ha abandonado en el nuevo artículo 197 *bis* 1, lo que en definitiva supone proteger en un solo precepto lo que en el caso español se tutelaba desde el año 2010, y se protege desde el 2015, en los citados artículos.

En cuanto a la expresa referencia a la tentativa dentro del mismo precepto, resulta coherente con la regulación unitaria que el legislador finlandés establece de estos delitos en un capítulo propio, en lugar de llevarla a la parte general como sucede en el caso español con la consiguiente dispersión de preceptos en torno a una misma conducta, pero no contempla los supuestos de mantenimiento en el sistema informático previsto en el artículo 197 *bis* 1 del Código español, conductas cuya inclusión, por otra parte, no viene impuesta por la normativa europea.

### *3.5 Hungría.*

En el ámbito húngaro la regulación penal de las conductas de *hacking* se encontraba en el artículo 300/C de su Código Penal de 1978, bajo la rúbrica relativa a crímenes contra la informática y sistemas de información. El citado precepto, tras la reforma de fecha 18 de diciembre de 2001, se refería al acceso no autorizado al sistema informático vulnerando las medidas de seguridad o la permanencia no autorizada dentro del sistema, incrementado en el mismo artículo las penas para los casos de daños en los datos u otras operaciones no

autorizadas en el sistema informático, o cuando el sujeto buscaba un enriquecimiento injusto con estas conductas, con mayores penas para los casos de graves daños, regulando los supuestos de facilitar el acceso en el artículo 300/E[243].

[243] La reforma de 18 de diciembre de 2001 establecía en los artículos 300/C y 300/E: "*Számítástechnikai rendszer és adatok elleni bűncselekmény. 300/C. §*

*(1) Aki számítástechnikai rendszerbe a számítástechnikai rendszer védelmét szolgáló intézkedés megsértésével vagy kijátszásával jogosulatlanul belép, vagy a belépési jogosultsága kereteit túllépve, illetőleg azt megsértve bent marad, vétséget követ el, és egy évig terjedő szabadságvesztéssel, közérdekű munkával vagy pénzbüntetéssel büntetendő.*

*(2) Aki*

*a) számítástechnikai rendszerben tárolt, feldolgozott, kezelt vagy továbbított adatot jogosulatlanul megváltoztat, töröl vagy hozzáférhetetlenné tesz,*

*b) adat bevitelével, továbbításával, megváltoztatásával, törlésével, illetőleg egyéb művelet végzésével a számítástechnikai rendszer működését jogosulatlanul akadályozza, vétséget követ el, és két évig terjedő szabadságvesztéssel, közérdekű munkával vagy pénzbüntetéssel büntetendő.*

*(3) Aki jogtalan haszonszerzés végett*

*a) a számítástechnikai rendszerbe adatot bevisz, az abban tárolt, feldolgozott, kezelt vagy továbbított adatot megváltoztat, töröl vagy hozzáférhetetlenné tesz, vagy*

*b) adat bevitelével, továbbításával, megváltoztatásával, törlésével, illetőleg egyéb művelet végzésével a számítástechnikai rendszer működését akadályozza, és ezzel kárt okoz, bűntettet követ el, és három évig terjedő szabadságvesztéssel büntetendő.*

*(4) A (3) bekezdésben meghatározott bűncselekmény büntetése*

*a) egy évtől öt évig terjedő szabadságvesztés, ha a bűncselekmény jelentős kárt okoz,*

*b) két évtől nyolc évig terjedő szabadságvesztés, ha a bűncselekmény különösen nagy kárt okoz,*

Por tanto, apenas hay un mes de diferencia entre el Convenio Europeo sobre Cibercriminalidad, aprobado por el Consejo de Europa el 23 de noviembre de 2001 y la regulación del *hacking* en el ordenamiento penal húngaro, si bien Hungría no firmaría el Convenio hasta el 4 de diciembre de 2003, razón por la cual estas conductas ya

---

*c) öt évtől tíz évig terjedő szabadságvesztés, ha a bűncselekmény különösen jelentős kárt okoz.*

Számítástechnikai rendszer védelmét biztosító technikai intézkedés kijátszása

*300/E. §*

*(1) Aki a 300/C. §-ban meghatározott bűncselekmény elkövetése céljából, az ehhez szükséges vagy ezt könnyítő számítástechnikai programot, jelszót, belépési kódot, vagy számítástechnikai rendszerbe való belépést lehetővé tevő adatot*

*a) készít,*

*b) megszerez,*

*c) forgalomba hoz, azzal kereskedik, vagy más módon hozzáférhetővé tesz, vétséget követ el, és két évig terjedő szabadságvesztéssel, közérdekű munkával vagy pénzbüntetéssel büntetendő.*

*(2) Az (1) bekezdés szerint büntetendő, aki a 300/C. §-ban meghatározott bűncselekmény elkövetése céljából az ehhez szükséges vagy ezt könnyítő, számítástechnikai program, jelszó, belépési kód, vagy valamely számítástechnikai rendszerbe való belépést lehetővé tevő adat készítésére vonatkozó gazdasági, műszaki, szervezési ismereteit másnak a rendelkezésére bocsátja.*

*(3) Nem büntethető az (1) bekezdés a) pontja esetén, aki – mielőtt a bűncselekmény elkövetéséhez szükséges vagy ezt megkönnyítő számítástechnikai program, jelszó, belépési kód, vagy valamely számítástechnikai rendszer egészébe vagy egy részébe való belépést lehetővé tevő adat készítése a hatóság tudomására jutott volna – tevékenységét a hatóság előtt felfedi, és az elkészített dolgot a hatóságnak átadja, valamint lehetővé teszi a készítésben részt vevő más személy kilétének megállapítását*", disponible en http://vpknet.vpk.bme.hu/doksik/szab_2.htm, consultado el 12 de enero de 2017.

estaban tipificadas en su Código con anterioridad a la citada ratificación.

Tras la aprobación del nuevo Código penal húngaro de fecha 13 de julio de 2012[244], la regulación del *hacking* se encuentra en el capítulo XLIII, relativo al acceso ilícito a datos y delitos contra sistemas de información, tipificando en su sección 422 las conductas en las que existe un propósito de acceder ilegalmente a datos personales, secretos privados o secretos comerciales[245], en su sección

---

[244] Código Penal de 13 de julio de 2012 disponible en http://net.jogtar.hu/jr/gen/hjegy_doc.cgi?docid=A1200100.TV, consultado el 12 de enero de 2017.

[245] "*422. § (1) Aki személyes adat, magántitok, gazdasági titok vagy üzleti titok jogosulatlan megismerése céljából*

*a) más lakását, egyéb helyiségét vagy az azokhoz tartozó bekerített helyet titokban átkutatja,*

*b) más lakásában, egyéb helyiségében vagy az azokhoz tartozó bekerített helyen történteket technikai eszköz alkalmazásával megfigyeli vagy rögzíti,*

*c) más közlést tartalmazó zárt küldeményét felbontja vagy megszerzi, és annak tartalmát technikai eszközzel rögzíti,*

*d) elektronikus hírközlő hálózat - ideértve az információs rendszert is - útján másnak továbbított vagy azon tárolt adatot kifürkész, és az észlelteket technikai eszközzel rögzíti, bűntett miatt három évig terjedő szabadságvesztéssel büntetendő.*

*(2) Az (1) bekezdés szerint büntetendő, aki fedett nyomozó vagy a bűnüldöző hatósággal, illetve titkosszolgálattal titkosan együttműködő személy kilétének vagy tevékenységének megállapítása céljából az (1) bekezdésben meghatározottakon kívül információt gyűjt.*

*(3) Az (1) bekezdés szerint büntetendő, aki az (1)-(2) bekezdésben meghatározott módon megismert személyes adatot, magántitkot, gazdasági titkot vagy üzleti titkot továbbít vagy felhasznál.*

*(4) A büntetés egy évtől öt évig terjedő szabadságvesztés, ha az (1)-(3) bekezdésben meghatározott tiltott adatszerzést*

423 los supuestos del acceso al sistema de información vulnerando las medidas de seguridad establecidas y los casos de daños[246] y, por último, en la sección 424 se tipifican los supuestos de facilitar las citadas conductas[247], de forma similar a la prevista en el artículo 197

---

*a) hivatalos eljárás színlelésével,*
*b) üzletszerűen,*
*c) bűnszövetségben vagy*
*d) jelentős érdeksérelmet okozva követik el*".

[246] "*Információs rendszer vagy adat megsértése- 423. (1) Aki információs rendszerbe az információs rendszer védelmét biztosító technikai intézkedés megsértésével vagy kijátszásával jogosulatlanul belép, vagy a belépési jogosultsága kereteit túllépve vagy azt megsértve bent marad, vétség miatt két évig terjedő szabadságvesztéssel büntetendő. (2) Aki a) az információs rendszer működését jogosulatlanul vagy jogosultsága kereteit megsértve akadályozza, vagy b) információs rendszerben lévő adatot jogosulatlanul vagy jogosultsága kereteit megsértve megváltoztat, töröl vagy hozzáférhetetlenné tesz, bűntett miatt három évig terjedő szabadságvesztéssel büntetendő. (3) A büntetés bűntett miatt egy évtől öt évig terjedő szabadságvesztés, ha a (2) bekezdésben meghatározott bűncselekmény jelentős számú információs rendszert érint. (4) A büntetés két évtől nyolc évig terjedő szabadságvesztés, ha a bűncselekményt közérdekű üzem ellen követik el. (5) E § alkalmazásában adat: információs rendszerben tárolt, kezelt, feldolgozott vagy továbbított tények, információk vagy fogalmak minden olyan formában való megjelenése, amely információs rendszer általi feldolgozásra alkalmas, ideértve azon programot is, amely valamely funkciónak az információs rendszer által való végrehajtását biztosítja*".

[247] "*Információs rendszer védelmét biztosító technikai intézkedés kijátszása - 424. Aki a 375. §-ban, a 422. § (1) bekezdés d) pontjában vagy a 423. §-ban meghatározott bűncselekmény elkövetése céljából az ehhez szükséges vagy ezt könnyítő a) jelszót vagy számítástechnikai programot készít, átad, hozzáférhetővé tesz, megszerez, vagy forgalomba hoz, illetve b) jelszó vagy számítástechnikai program készítésére vonatkozó gazdasági, műszaki, szervezési ismereteit más rendelkezésére bocsátja, vétség miatt két évig terjedő szabadságvesztéssel büntetendő. (2) Nem büntethető az (1) bekezdés a) pontjában meghatározott bűncselekmény elkövetője, ha -*

*ter* del Código español.

Por tanto, el Código húngaro distingue entre el acceso a datos y el acceso a sistemas de información, que regula en preceptos separados y sin establecer un concepto previo como sucede en el Convenio Europeo sobre Cibercriminalidad, la DM 2005/222/JAI, o la Directiva 2013/40/UE, incorporando la necesaria vulneración de medidas de seguridad para el acceso al sistema de información, tal y como exige el artículo 3 de la Directiva, y sin incluir los supuestos de mantenimiento en el sistema de información que incluye el Código español. Sin embargo, es destacable la labor sistemática del legislador húngaro, que, en la nueva regulación de estas conductas, las ubica bajo un mismo capítulo, relativo al acceso ilícito a datos y delitos contra sistemas de información, acorde con la creciente criminalidad en torno a las nuevas tecnologías que exige dotar de un tratamiento autónomo estos delitos.

---

*mielőtt a bűncselekmény elkövetéséhez szükséges vagy ezt megkönnyítő jelszó vagy számítástechnikai program készítése a büntető ügyekben eljáró hatóság tudomására jutott volna - tevékenységét a hatóság előtt felfedi, az elkészített dolgot a hatóságnak átadja, és lehetővé teszi a készítésben részt vevő más személy kilétének megállapítását. (3) E § alkalmazásában jelszó: az információs rendszerbe vagy annak egy részébe való belépést lehetővé tevő, számokból, betűkből, jelekből, biometrikus adatokból vagy ezek kombinációjából álló bármely azonosító*".

## *4. PAÍSES QUE REGULAN EL DELITO DE HACKING JUNTO A OTROS DELITOS.*

Se incluye en este epígrafe la normativa de los Estados europeos que, como España, han optado por tipificar el delito de *hacking* junto a otros delitos que tutelan bienes jurídicos diversos a los de estas conductas, tal y como veremos en el siguiente Capítulo. Dentro de este grupo se encuentran la mayoría de países de nuestro entorno. En concreto, Alemania, Austria, Dinamarca, Eslovaquia, Eslovenia, Estonia, Francia, Grecia, Holanda, Irlanda, Italia, Letonia, Lituania, Luxemburgo, Malta, Polonia, República Checa, Rumanía y Suecia.

A continuación se hace una breve referencia a sus legislaciones con mención a los delitos entre los que se sitúan al *hacking* y algunas de sus diferencias con la regulación española, a la que se dedican los siguientes Capítulos del trabajo.

### *4.1 Alemania.*

Como consecuencia de la enmienda introducida en fecha 7 de agosto de 2007[248], dentro del Capítulo Decimoquinto del StGB

[248] Einundvierzigstes Strafrechtsänderungsgesetz zur Bekämpfung der Computerkriminalität (41. StrÄndG), tal y como se dispone en su encabezamiento, la reforma introducida por esta Ley estaba dirigida a

alemán[249], dedicada a la violación de la vida personal y el área secreta, se regulan en su parágrafo § 202a las conductas de espionaje, donde se comprende el acceso no autorizado a datos protegidos superando las medidas de seguridad de acceso. En concreto, según su punto segundo, se castiga el acceso a los datos almacenados o transmitidos electrónicamente, magnéticamente o por cualquier otra forma no inmediatamente perceptible[250]. Todo ello, sin referirse al mantenimiento no autorizado en el sistema.

De esta forma, al igual que en el Código Penal español, en el ámbito alemán se regula el acceso no autorizado vulnerando medidas

---

poner en práctica la DM 2005/222/JAI. Reforma disponible en http://www.buzer.de/gesetz/7846/, consultado el 20 de septiembre de 2016.

[249] Código penal de 15 de mayo de 1871, con sus reformas, disponible en https://www.gesetze-im-internet.de/stgb/, consultado el 20 de septiembre de 2016.

[250] *"§ 202a Ausspähen von Daten. (1) Wer unbefugt sich oder einem anderen Zugang zu Daten, die nicht für ihn bestimmt und die gegen unberechtigten Zugang besonders gesichert sind, unter Überwindung der Zugangssicherung verschafft, wird mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe bestraft. (2) Daten im Sinne des Absatzes 1 sind nur solche, die elektronisch, magnetisch oder sonst nicht unmittelbar wahrnehmbar gespeichert sind oder übermittelt werden.".* En su version inglesa, disponible en http://www.gesetze-im-internet.de/englisch_stgb/index.html, consultado el 20 de septiembre de 2016, *"Section 202a Data espionaje. (1) Whosoever unlawfully obtains data for himself or another that were not intended for him and were especially protected against unauthorised access, if he has circumvented the protection, shall be liable to imprisonment not exceeding three years or a fine. (2) Within the meaning of subsection (1) above data shall only be those stored or transmitted electronically or magnetically or otherwise in a manner not immediately perceivable.".*

de seguridad, pero con la peculiaridad de estar relacionado con datos protegidos, de forma similar a la establecida en el artículo 197.3 CP tras la reforma de la LO 5/2010, relativa al acceso a datos. Así pues, la regulación alemana se aleja de la actual conducta prevista en el artículo 197 *bis* 1 CP, que tras la reforma de la LO 1/2015 viene referido a todo o parte del sistema de información, y no incluye referencia alguna a las conductas de permanencia en el sistema, que se mantienen en el Código español desde la introducción de estos delitos con la LO 5/2010.

La tipificación del acceso a datos en el StGB alemán, tal y como sucedía con la redacción dada al artículo 197.3 del Código Penal español por la LO 5/2010, no es acorde con las previsiones de los artículos 2 y 3, respectivamente, de la DM 2005/222/JAI y la Directiva 2013/40/UE, que mencionan el mero acceso al conjunto o una parte de un sistema de información sin referirse a los datos en ellos contenidos.

Por tanto, en el ámbito alemán el precepto no protege cualquier sistema, dato o programa, frente a un supuesto acceso no autorizado, sino tan sólo datos almacenados o transmitidos electrónicamente, magnéticamente o por cualquier otra forma no inmediatamente perceptible.

Por último, en relación con las conductas de *hacking* se dedica el parágrafo § 202c[251] a los actos preparatorios en relación al delito de

[251] *"§ 202c Vorbereiten des Ausspähens und Abfangens von Daten*

acceso a los datos mencionado, mediante la producción, adquisición para sí o para otro, venta, suministro, difusión o haciendo accesible contraseñas u otros códigos de seguridad que permitan el acceso a los datos, o *software* con el propósito de la comisión de ese delito, de modo similar al 197 *ter* del Código penal español, introducido tras la reforma de la LO 1/2015 y que se expondrá en el Capítulo IV del presente trabajo.

Es destacable que el legislador alemán no haya optado por una regulación unitaria de los delitos informáticos sino, como la mayoría de países europeos, por su regulación en una sección junto a otros delitos de distinta naturaleza, en este caso, delitos relativos a la violación de la vida personal y el área secreta, es decir, dentro de la

---

*(1) Wer eine Straftat nach § 202a oder § 202b vorbereitet, indem er*

*1. Passwörter oder sonstige Sicherungscodes, die den Zugang zu Daten (§ 202a Abs. 2) ermöglichen, oder*

*2. Computerprogramme, deren Zweck die Begehung einer solchen Tat ist,*

*herstellt, sich oder einem anderen verschafft, verkauft, einem anderen überlässt, verbreitet oder sonst zugänglich macht, wird mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft.*

*(2) § 149 Abs. 2 und 3 gilt entsprechend.".*

En su versión inglesa, el precepto establece: "*Section 202c Acts preparatory to data espionage and phishing. (1) Whosoever prepares the commission of an offence under section 202a or section 202b by producing, acquiring for himself or another, selling, supplying to another, disseminating or making otherwise accessible*

*1. passwords or other security codes enabling access to data (section 202a(2)), or*

*2. software for the purpose of the commission of such an offence, shall be liable to imprisonment not exceeding one year or a fine.*

*(2) Section 149(2) and (3) shall apply mutatis mutandis."*.

categoría de conductas que atentan contra la intimidad, tal y como sucede en el caso español. Esto plantea en principio los mismos problemas interpretativos que en nuestro ordenamiento para los supuestos en que los datos a los que se accede no afecten a la intimidad. Por ello, habría sido deseable un tratamiento diferenciado respecto a estos delitos estableciendo una sección propia destinada a la tutela de la integridad o la seguridad de los datos a los que se refiere el precepto.

### *4.2 Austria.*

El Código penal austríaco de 1974, tras la reforma del año 2002, contiene la definición de sistemas informáticos en su artículo 74.8[252], que en traducción libre pueden entenderse como aquéllos dispositivos, individuales o asociados, que permiten el procesamiento automatizado de datos, siguiendo así la línea del artículo 1.a) de la DM 2005/222/JAI y del artículo 2.a) de la Directiva 2013/40/UE, aunque más cercana por su sencillez a la definición del artículo 1 del Convenio Europeo sobre Cibercriminalidad, ratificado por Austria el

[252] El parágrafo 74.8 del Código penal austriaco, introducido por la Ley 134/2002, de 13 de agosto, contiene como definición "*§ 74. (1) Im Sinn dieses Bundesgesetzes ist* (…) *8. Computersystem: sowohl einzelne als auch verbundene Vorrichtungen, die der automationsunterstützten Datenverarbeitung dienen;*", Ley disponible en https://www.ris.bka.gv.at/Dokumente/BgblPdf/2002_134_1/2002_134_1.pdf, consultado el 12 de enero de 2017.

13 de junio de 2012.

Con la citada modificación del año 2002, el parágrafo 118a[253] del Código regulaba las conductas de *hacking* dentro de la Sección Quinta, dedicada a las violaciones de la privacidad y de ciertos secretos profesionales, bajo la rúbrica relativa al acceso ilícito a un sistema informático, castigando el acceso no autorizado a datos almacenados en todo o parte de un sistema informático con daño a la medida específica de seguridad del sistema, incluyendo con las mismas penas la puesta a disposición de los datos a favor de terceros. De esta forma, al igual que en el caso del StGB alemán, se equipara a las conductas de acceso a datos que estaban tipificadas en el artículo 197.3 del Código español tras la reforma de la LO 5/2010 hasta la reforma de la LO 1/2015.

---

[253] El parágrafo 118a del Código penal austriaco, en su redacción introducida por la Ley de 13 de agosto de 2002, establecía: "*Widerrechtlicher Zugriff auf ein Computersystem. § 118a. (1) Wer sich in der Absicht, sich oder einem anderen Unbefugten von in einem Computersystem gespeicherten und nicht für ihn bestimmten Daten Kenntnis zu verschaffen und dadurch, dass er die Daten selbst benützt, einem anderen, für den sie nicht bestimmt sind, zugänglich macht oder veröffentlicht, sich oder einem anderen einen Vermögensvorteil zuzuwenden oder einem anderen einen Nachteil zuzufügen, zu einem Computersystem, über das er nicht oder nicht allein verfügen darf, oder zu einem Teil eines solchen Zugang verschafft, indem er spezifische Sicherheitsvorkehrungen im Computersystem verletzt, ist mit Freiheitsstrafe bis zu sechs Monaten oder mit Geldstrafe bis zu 360 Tagessätzen zu bestrafen. (2) Der Täter ist nur mit Ermächtigung des Verletzten zu verfolgen.*".
Código Penal austriaco, de 23 de enero de 1974, disponible en https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=10002296, consultado el 12 de enero de 2017.

La Ley de 109/2007, de 28 de diciembre de 2007, modifica el parágrafo 118a del Código penal, sustituyendo el término relativo al daño en las medidas de seguridad por el referente a la superación de las medidas de seguridad, e introduce un tercer párrafo, en el que se establecen mayores penas en los supuestos en que el sujeto sea miembro de una organización criminal. En este último caso, sin distinguir entre grupo y organización, es decir, tal y como ha optado el legislador español en el artículo 197 *quater* del Código penal[254], introducido tras la reforma de la LO 1/2015 y que veremos en el Capítulo V. Todo ello, sin incluir además las conductas de mantenimiento en el sistema comprendidas en el Código español desde la LO 5/2010.

Por tanto, en el Código austríaco destaca el establecimiento de definiciones previas en el citado parágrafo 74, como son inmadurez, minoría de edad, oficial, funcionario, oficial de la Comunidad, árbitro, amenaza peligrosa, tarifa, certificado, el citado sistema informático, prostitución, o infraestructura crítica, que facilitan la interpretación de estos delitos, pero se opta por tipificar el *hacking* junto a otros delitos contra la privacidad y secretos profesionales, con el consiguiente problema interpretativo que plantea en torno al bien jurídico

[254] La Ley de 28 de diciembre de 2007 establece en su artículo I.11: "*11. § 118a wird wie folgt geändert: a) Im Abs. 1 wird das Wort „verletzt" durch das Wort „überwindet" ersetzt. b) Nach dem Abs. 2 wird folgender Abs. 3 angefügt: „(3) Wer die Tat als Mitglied einer kriminellen Vereinigung begeht, ist mit Freiheitsstrafe bis zu drei Jahren zu bestrafen*", disponible en https://www.ris.bka.gv.at/Dokumente/BgblAuth/BGBLA_2007_I_109/BGBLA_2007_I_109.pdf, consultado el 12 de enero de 2017.

protegido, problema similar al del Código español, tal y como se expondrá en el siguiente Capítulo.

### *4.3 Dinamarca.*

En el ámbito danés el Código penal de 27 de septiembre de 2005[255], tras la reforma de 21 de diciembre del mismo año, contiene las conductas de *hacking* en el artículo 263, ubicado en el capítulo 27 dedicado a los delitos contra el honor y ciertos derechos individuales, de su parte especial.

En concreto, su apartado 2 establece la pena para el que ilegalmente obtiene acceso a la información de otra persona o a programas diseñados para ser utilizados en un sistema de información, incrementándose las penas en el apartado 3 para los casos en que exista la intención de adquirir o procurar información relativa a secretos de empresa o en casos especialmente graves[256]. De esta

---

[255] Disponible en https://www.retsinformation.dk/Forms/R0710.aspx?id=2406, y en https://www.unodc.org/tldb/pdf/Denmark_Criminal_Code_2005.pdf, en su versión inglesa, consultado el 12 de enero de 2017.

[256] *"27. Kapitel Freds- og ærekrænkelser § 263. (…)*
*Stk. 2. Med bøde eller fængsel indtil 1 år og 6 måneder straffes den, der uberettiget skaffer sig adgang til en andens oplysninger eller programmer, der er bestemt til at bruges i et informationssystem.*
*Stk. 3. Begås de i stk. 1 eller 2 nævnte forhold med forsæt til at skaffe sig eller gøre sig bekendt med oplysninger om en virksomheds erhvervshemmeligheder eller under andre særligt skærpende*

forma, se castiga el acceso a la información o programas, lo que equivaldría a la regulación del artículo 197.3 del Código español tras la reforma de la LO 5/2010.

Por su parte, el artículo 263a[257] establece en su primer párrafo

---

*omstændigheder, kan straffen stige til fængsel indtil 6 år. På samme måde straffes de i stk. 2 nævnte forhold, når der er tale om overtrædelser af mere systematisk eller organiseret karakter.".*

En su version inglesa: "*Chapter 27 Offences against Personal Honour and Certain Individual Rights*
*§ 263 (2) Any person who unlawfully obtains access to another person's information or programmes designated for use in an information system shall be liable to a fine or to imprisonment for any term not exceeding one year and six months. (3) If the acts mentioned in Subsections (1) and (2) above are committed with the intent to procure or make oneself acquainted with information about trade secrets of a firm, or in other particularly aggravating circumstances, the penalty may be increased to imprisonment for any term not exceeding six years. This penalty also applies to the acts described in Subsection (2) above in the case of offences of a more systematic or organised nature*.".

[257] "*§ 263 a. Med bøde eller fængsel indtil 1 år og 6 måneder straffes den, der uretmæssigt erhvervsmæssigt sælger eller i en videre kreds udbreder en kode eller andet adgangsmiddel til et ikke offentligt tilgængeligt informationssystem, hvortil adgangen er beskyttet med kode eller anden særlig adgangsbegrænsning.*
*Stk. 2. På samme måde straffes den, der uretmæssigt videregiver et større antal koder eller andre adgangsmidler som nævnt i stk. 1.*
*Stk. 3. På samme måde straffes den, der uretmæssigt skaffer sig eller videregiver en kode eller andet adgangsmiddel som nævnt i stk. 1 til*

*1) et samfundsvigtigt informationssystem, jf. § 193, eller*

*2) et informationssystem, der behandler følsomme oplysninger, som er omfattet af § 7, stk. 1, eller § 8, stk. 1, i lov om behandling af personoplysninger, om flere personers personlige forhold.*

*Stk. 4. Sker den i stk. 1-3 nævnte videregivelse m.v. under særligt skærpende omstændigheder, er straffen fængsel indtil 6 år. Som særligt*

las penas para el que ilegalmente comercialice o difunda contraseñas o medios de acceso a un sistema de información no público cuyo acceso está protegido por un código u otra restricción de acceso, similar al actual artículo 197 *ter* CP, imponiendo la misma pena su apartado 2 para quien redistribuya un gran número de códigos u otros medios de acceso mencionados en el apartado primero, y en el apartado 3 se establece la pena para quien disponga o transmita un código u otros medios de acceso a una información importante para la comunidad o a un sistema de información que se ocupa de información sensible, concluyendo el apartado 4 con las agravantes en supuestos de especial importancia o un riesgo de daño significativo.

---

*skærpende omstændigheder anses navnlig tilfælde, hvor videregivelsen m.v. sker i særlig stort omfang eller indebærer særlig risiko for betydelig skade.".*

En su version inglesa: *"§ 263 a (1) Any person who, in an unlawful manner, commercially sells or widely disseminates a password or other means of access to an information system, which is not accessible to the public and to which access is secured by a password or other special access restrictions, shall be liable to a fine or to imprisonment for any term not exceeding one year and six months. (2) Similar punishment shall apply to any person who unlawfully passes on a greater number of passwords or other means of access as mentioned in Subsection (1) above. (3) Similar punishment shall apply to any person who unlawfully obtains or passes on a password or other means of access as mentioned in Subsection (1) above to I) an information system of national importance, cf. Section 193 of this Act; or 2) an information system, which handles sensitive information of the kind included under Section 711) or Section 8(L) of the Law concerning Handling of Personal Information, about several people's personal circumstances. (4) If the passing on etc., as mentioned in Subsections (1)-(3) above, takes place under particularly aggravating circumstances, the penalty shall be imprisonment for any term not exceeding six years. Considered as particularly aggravating circumstances are especially instances where the passing on etc. has occurred to a particularly great extent or implies a distinct risk of considerable damage.".*

Por último, en relación con las conductas de *hacking*, el artículo 264c[258] establece las penas para el que sin haber participado en los delitos, obtiene o ilegalmente explota la información obtenida por medio de ellos.

Por tanto, aunque el Código danés se ocupa de las conductas de *hacking* en relación con el acceso a datos o programas informáticos, sin embargo, no contempla los supuestos de mantenimiento en el sistema como se incluye en el Código español, ni exige que se quebranten las medidas de seguridad en el acceso al sistema de información que establece el artículo 3 de la Directiva 2013/40/UE. El Código danés tipifica estos hechos entre los delitos contra el honor y otros derechos individuales, por lo que tampoco establece un capítulo propio para el acceso a los sistemas informáticos o los delitos informáticos, que aportaría claridad en la interpretación de los preceptos. No obstante, destaca en este Código la tipificación de los distintos supuestos y circunstancias en torno al tipo básico del artículo 263.2, al que le siguen las citadas conductas dentro del mismo capítulo como serían las del artículo 264.c, donde tendría cabida la receptación, que en nuestro caso se regula de forma dispersa a la

[258] El parágrafo establece *"§ 264 c. De i §§ 263, 264 og 264 a indeholdte straffebestemmelser finder tilsvarende anvendelse på den, der uden at have medvirket til gerningen skaffer sig eller uberettiget udnytter oplysninger, som er fremkommet ved overtrædelsen*."

En su version inglesa: *"§ 264 c The penal provisions contained in Sections 263, 264 and 264 a of this Act shall similarly apply to any person who, without having participated in the act in question, obtains or unlawfully exploits information which has been brought to light by the offence*".

regulación del *hacking* en los artículo 298 a 304 CP.

### *4.4 Eslovaquia.*

La tipificación del *hacking* en el caso de Eslovaquia se encuentra en la sección 247 de su Código Criminal de 2 de julio de 2005[259], dentro del capítulo cuarto de su parte especial, dedicado a los delitos contra el derecho de propiedad.

El precepto lleva la rúbrica relativa al acceso no autorizado al sistema informático, regulando en su primer apartado las conductas del acceso ilegal a un sistema de información o parte del mismo vulnerando las medidas de seguridad establecidas, siguiendo lo dispuesto en el artículo 3 de la Directiva 2013/40/UE, tal y como establece también el artículo 197 *bis* 1 del Código Penal español si bien, a diferencia de este precepto, no incluye expresamente las conductas de mantenimiento no autorizado en el sistema informático.

Las penas se agravan en el apartado 2 si se causan daños

[259] La sección 247 establece: "*§ 247 Neoprávnený prístup do počítačového systému (1) Kto prekoná bezpečnostné opatrenie, a tým získa neoprávnený prístup do počítačového systému alebo jeho časti, potrestá sa odňatím slobody až na dva roky. (2) Odňatím slobody na jeden rok až päť rokov sa páchateľ potrestá, ak spácha čin uvedený v odseku 1 a spôsobí ním značnú škodu. (3) Odňatím slobody na tri roky až osem rokov sa páchateľ potrestá, ak spácha čin uvedený v odseku 1 a) a spôsobí ním škodu veľkého rozsahu, alebo b) ako člen nebezpečného zoskupenia*", disponible en http://www.zakonypreludi.sk/zz/2005-300, consultado el 12 de enero de 2017.

sustanciales, incluyendo por tanto los daños a sistemas informáticos en el mismo artículo, y se establece mayor castigo en el apartado 3 para los supuestos en los que los daños son importantes o el sujeto es miembro de una agrupación peligrosa, regulando en este último caso, también en el mismo precepto, los supuestos de organización o grupo criminal que en el Código español se llevan al artículo 197 *quater*, tal y como veremos en el Capítulo V.

Por su parte, el artículo 247a[260] regula los supuestos que denomina en su rúbrica de intrusismo. En concreto, en su apartado 1 establece el tipo básico comprendiendo la conducta de cualquier persona que limite o interrumpa el funcionamiento de todo o parte de un sistema informático con una entrada no autorizada, transmisión, daño, borrado, deterioro, alteración, supresión o haciendo inaccesibles los datos, o que haga una modificación no autorizada del *hardware* o

---

260 *"§ 247a Neoprávnený zásah do počítačového systému (1) Kto obmedzí alebo preruší fungovanie počítačového systému alebo jeho časti a) neoprávneným vkladaním, prenášaním, poškodením, vymazaním, zhoršením kvality, pozmenením, potlačením alebo zneprístupnením počítačových údajov, alebo b) tým, že urobí neoprávnený zásah do technického alebo programového vybavenia počítača a získané informácie neoprávnene zničí, poškodí, vymaže, pozmení alebo zníži ich kvalitu, potrestá sa odňatím slobody na šesť mesiacov až tri roky. (2) Odňatím slobody na tri roky až osem rokov sa páchateľ potrestá, ak spácha čin uvedený v odseku 1 a) a spôsobí ním značnú škodu, b) a spôsobí ním vážnu poruchu v činnosti štátneho orgánu, orgánu územnej samosprávy, súdu alebo iného orgánu verejnej moci, c) tak, že zneužije osobné údaje iného s cieľom získať dôveru tretej strany. (3) Odňatím slobody na štyri roky až desať rokov sa páchateľ potrestá, ak spácha čin uvedený v odseku 1 a) a spôsobí ním škodu veľkého rozsahu, b) a spôsobí ním vážnu poruchu v kritickej infraštruktúre, alebo c) ako člen nebezpečného zoskupenia".*

*software*, y la información obtenida ilegalmente destruya, dañe, suprima, altere o reduzca su calidad.

El apartado 2 incrementa las penas en los supuestos de daños significativos, grave perturbación en la actividad de una autoridad pública, o en los casos de explotación de datos personales de otros para ganar la confianza de un tercero.

Por último, el apartado 3 establece mayor castigo para los casos en los que la conducta del apartado 1 cause un daño importante, provoque una grave perturbación de una infraestructura crítica o el sujeto sea miembro de una agrupación peligrosa.

En relación con las citadas conductas de *hacking*, el artículo 247d[261] tipifica la producción y posesión de dispositivos de acceso o contraseñas para el sistema informático u otros datos en relación con los citados supuestos de los artículos 247 y 247a, castigando al que

[261] *"§ 247d Výroba a držba prístupového zariadenia, hesla do počítačového systému alebo iných údajov (1) Kto v úmysle spáchať trestný čin neoprávneného prístupu do počítačového systému podľa § 247, neoprávneného zásahu do počítačového systému podľa § 247a, neoprávneného zásahu do počítačového údaja podľa § 247b alebo neoprávneného zachytávania počítačových údajov podľa § 247c vyrobí, dovezie, obstará, kúpi, predá, vymení, uvedie do obehu alebo akokoľvek sprístupní a) zariadenie vrátane počítačového programu vytvorené na neoprávnený prístup do počítačového systému alebo jeho časti, alebo b) počítačové heslo, prístupový kód alebo podobné údaje umožňujúce prístup do počítačového systému alebo jeho časti, potrestá sa odňatím slobody až na dva roky. (2) Odňatím slobody na šesť mesiacov až tri roky sa páchateľ potrestá, ak spácha čin uvedený v odseku 1 a spôsobí ním značnú škodu. (3) Odňatím slobody na jeden rok až päť rokov sa páchateľ potrestá, ak spácha čin uvedený v odseku 1 a) a spôsobí ním škodu veľkého rozsahu, alebo b) ako člen nebezpečného zoskupenia".*

fabrica, importa, adquiere, compra, vende, intercambia, pone en circulación o hace disponible de cualquier manera un dispositivo, incluso un programa informático para obtener el acceso no autorizado, o bien una contraseña de ordenador, código de acceso, o datos similares para permitir el acceso al sistema informático o parte del mismo, de forma similar al artículo 197 *ter* del Código español.

Las penas se incrementan en su apartado 2 para el caso de daños sustanciales y en el apartado 3 para los supuestos de daños mayores o si el sujeto es miembro de un grupo peligroso.

Por tanto, aunque el Código eslovaco no incluye definiciones previas de los conceptos relativos al delito de *hacking* como en los instrumentos internacionales, sí que se ocupa de su regulación cumpliendo las exigencias que ha establecido posteriormente el artículo 3 de la Directiva 2013/40/UE en materia de vulneración de medidas de seguridad. No obstante, como los otros Códigos europeos incluidos en este grupo, el legislador tampoco se ha preocupado de tipificar estos delitos en un título propio, donde se podrían haber incluido los delitos informáticos. En su lugar, se ha optado por regularlo en un capítulo en el que incluye otros delitos contra la propiedad, obviando la importancia y sustantividad propia de los ciberdelitos y con el consiguiente riesgo de confusión entre bienes jurídicos protegidos.

### *4.5 Eslovenia.*

En el ámbito esloveno el delito de *hacking* se encuentra tipificado en el artículo 225 de su Código Penal[262] bajo la rúbrica relativa a la entrada no autorizada en el sistema de información, ubicado en el capítulo veintitrés de su parte especial, dedicado a los delitos contra la propiedad.

El legislador ha tipificado en un mismo precepto el delito de *hacking* y los daños o interferencias en los sistemas informáticos.

En concreto, el primer apartado del artículo 225 establece las penas para el que sin estar autorizado entra en un sistema de información o intercepta indebidamente datos de naturaleza no pública que están siendo transferidos hacia o desde un sistema de información. Es decir, no se exige la vulneración de medidas de seguridad para la comisión del delito, siguiendo el criterio del Convenio Europeo sobre

---

[262] El Código penal de la República de Eslovenia de 27 de agosto de 2004 establece en su artículo 225: "*Nepravičen vstop v informacijski sistema 225. člen (1) Kdor nepravičeno vstopi v informacijski sistem ali kdor nepravičeno prestreže podatek ob nejavnem prenosu v ali iz informacijskega sistema, se kaznuje z denarno kaznijo.(2) Kdor podatke v informacijskem sistemu nepravičeno uporabi, spremeni, preslika, prenaša, uniči ali v informacijski sistem nepravičeno vnese kakšen podatek, ovira prenos podatkov ali delovanje informacijskega sistema, se kaznuje za zaporom do dveh let. (3) Poskus dejanja iz prejšnjega odstavka je kazniv.*
*(4) Če je z dejanjem iz drugega odstavka tega člena povzročena velika škoda, se storilec kaznuje z zaporom od treh mesecev do petih let.*", disponible en http://www2.gov.si/up-rs/2002-2007/jd.nsf/dokumentiweb/D4B6CCF32BB7E8A3C1256F94000A952D?OpenDocument, consultado el 12 de enero de 2017.

Cibercriminalidad y la DM 2005/222/JAI, y apartándose de la previsión del artículo 3 de la Directiva 2013/40/UE que exige que el acceso "*se haya cometido con violación de una medida de seguridad*", vulneración que se contempla en el artículo 197 *bis* 1 del Código Penal español.

Por su parte, el apartado segundo del precepto castiga el uso, cambio, copia, transferencia o destrucción de datos mantenidos en un sistema de información, de forma no autorizada, o la introducción de datos u obstrucción en la transferencia de datos de un sistema de información, también de forma no autorizada.

Por último, se contempla la tentativa del delito en su apartado 3, lo que supone su tipificación expresa en la parte especial a diferencia del Código español que la regula en sus artículos 16 y 62, y se concluye con el apartado 4 dedicado a la agravante consistente en que se causen daños importantes con la comisión de estos delitos.

Por tanto, en el caso de Eslovenia, al igual que en Eslovaquia, el legislador ha optado por ubicar estos delitos entre los delitos contra la propiedad, surgiendo el problema de delimitación del bien jurídico protegido, tal y como acontece en el Código español al regularlas entre los delitos contra la intimidad, problemática que se expondrá en el Capítulo III.

### *4.6 Estonia.*

En Estonia la regulación penal de las conductas de *hacking* se encuentra en el artículo 217 de su Código penal[263] tras la reforma llevada a cabo por la norma denominada RT I, 12.07.2014, 1. La rúbrica del precepto se refiere al acceso ilegal a los sistemas informáticos y se ubica en la subdivisión 3 dedicada a los usos ilegales, de la división 2 que regula los delitos contra todo tipo de propiedad, del capítulo 13 relativo a los delitos contra la propiedad, de su parte especial.

El artículo viene precedido del 216, donde se tipifica la preparación del delito relacionado con el sistema informático, castigando de forma similar al artículo 197 *ter* del Código español, el suministro, producción, posesión, distribución u otra forma de puesta

---

[263] El artículo 217 del Código penal estonio, en su versión en inglés: "*"§ 217. Illegal obtaining of access to computer systems (1) Illegal obtaining of access to computer systems by elimination or avoidance of means of protection*
*is punishable by a pecuniary punishment or up to three years' imprisonment. (2) The same act:*
*1) if it causes significant damage; or 2) if access was obtained to a computer system containing a state secret, classified foreign information or information prescribed for official use only; or 3) if access was obtained to a computer system of a vital sector,*
*is punishable by a pecuniary punishment or up to five years' imprisonment. (3) An act provided for in subsection (1) or (2) of this section, if committed by a legal person, is punishable by a pecuniary punishment",* disponible en https://www.riigiteataja.ee/en/eli/522012015002/consolide, consultado el 12 de enero de 2017.

a disposición de un programa de ordenador o dispositivo que se crea o se ajusta, en particular, para la comisión de los delitos previstos en los artículos 206, 207, 213 o 217, o de los medios de protección que permiten obtener acceso a un sistema informático con la intención de obtener su propio provecho o permitiendo a un tercero la comisión de esos delitos.

En el caso del artículo 217, se castiga el acceso ilícito al sistema informático eliminando o eludiendo las medidas de seguridad, de forma similar al Código español.

Las penas se incrementan en el mismo precepto para los casos de daños informáticos o si se trata de sistemas informáticos que contienen secretos de Estado, información extranjera clasificada o información oficial, o si el acceso es para usar los datos contenidos en el sistema informático, estableciendo una pena todavía mayor en los supuestos en que el acceso sea a un sistema informático crítico y pena de multa en los casos en que las conductas son realizadas por personas jurídicas.

Por tanto, no se regula el mantenimiento en el sistema informático como ocurre en el caso del artículo 197 *bis* 1 del Código penal español y hay expresa referencia a la vulneración de las medidas de seguridad, reflejando este punto el elemento al que daba libertad el artículo 2 del Convenio Europeo sobre Cibercriminalidad, aprobado por el Consejo de Europa el 23 de noviembre de 2001 y ratificado por Estonia el 12 de mayo de 2003, y el artículo 2.2 de la DM 2005/222/JAI, circunstancia que se viene exigiendo en las

legislaciones internas desde el citado artículo 3 de la Directiva 2013/40/UE.

Si bien, al igual que en los casos de Eslovaquia y Eslovenia, el Código estonio vuelve a ubicar el delito de *hacking* entre los delitos contra la propiedad, es destacable que el legislador haya dado un paso más y haya establecido una subdivisión específica a lo que denomina usos ilegales, agrupando tanto el uso no autorizado de cosas muebles, de electricidad, gas o energía térmica, como el acceso a los sistemas informáticos, de forma que dota de una autonomía relativa a estos delitos al dedicarles una subdivisión propia, si bien bajo la rúbrica de los delitos contra la propiedad.

### *4.7 Francia.*

Aunque en fecha 10 de enero de 2006[264] Francia firmó el Convenio Europeo sobre Cibercriminalidad, lo cierto es que desde 1988 el acceso ilícito a los sistemas informáticos ya estaba tipificado en el Código penal francés[265].

---

[264] La lista de Estados firmantes del Convenio, con las fechas de ratificaciones y entrada en vigor, se encuentra disponible en http://www.coe.int/es/web/conventions/full-list/-/conventions/treaty/185/signatures?p_auth=LdzvnXOk, consultado el 12 de enero de 2017.

[265] El artículo 462-2 del Código penal francés, fue introducido por la LOI nº 88-19 du 5 janvier 1988, relative à la fraude informatique (1), donde se establecía "*Quiconque, frauduleusement, aura accédé ou se será maintenu*

El citado Código[266] dedica actualmente su artículo 323-1 a las conductas de *hacking* dentro del libro III, que regula los crímenes y delitos contra la propiedad, título II relativo a otros daños a la propiedad, capítulo III dedicado a los ataques a los sistemas de tratamiento automatizado de datos, y la redacción vigente del citado artículo ha sido introducida por la Ley 2015-912 de 24 de julio de 2015, relativa a la información[267].

En concreto, el precepto regula el *hacking* en su primer párrafo, castigando los atentados contra los sistemas automatizados de datos, en el que se incluye tanto el acceso como la permanencia de forma fraudulenta en la totalidad del sistema, y establece mayores penas en su párrafo segundo para los supuestos en que se causa la eliminación o modificación de datos en el sistema o su funcionamiento deteriorado[268].

---

*dans tout ou partie d'un système de traitement automatisé de données sera puni d'un emprisonnement de deux mois à un an et d'une amende de 2000 F à 50000 F ou de l'une de ces deux peines*", disponible en http://www.legifrance.gouv.fr/jopdf/common/jo_pdf.jsp?numJO=0&dateJO=19880106&numTexte=&pageDebut=00231&pageFin=00231, consultado el 12 de enero de 2017.

[266] Disponible en http://www.legifrance.gouv.fr/affichCode.do;jsessionid=EBB6E17DE38CA5F61DF90B20DFA6AED6.tpdila08v_1?idSectionTA=LEGISCTA000006149839&cidTexte=LEGITEXT000006070719&dateTexte=20151027, consultado el 12 de enero de 2017.

[267] LOI n° 2015-912 du 24 juillet 2015 relative au renseignement (1), disponible en http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000030931899&categorieLien=id, consultado el 12 de enero de 2017.

[268] *"Article 323-1*

*Le fait d'accéder ou de se maintenir, frauduleusement, dans tout ou*

Por tanto, al igual que en Código español, en el caso francés el legislador se ocupa del acceso y mantenimiento en todo o parte del sistema informático, si bien no hay referencia expresa a la vulneración de medidas de seguridad ni a la ausencia de autorización, a los que se refiere el artículo 3 de la Directiva 2013/40/UE, sino que se opta por el término "*frauduleusement*", es decir, acceder o mantenerse en el sistema fraudulentamente, concepto que incluye tanto los supuestos de cualquier indicación contraria al acceso como la vulneración de medidas de seguridad[269].

---

*partie d'un système de traitement automatisé de données est puni de deux ans d'emprisonnement et de 60 000 € d'amende.*

*Lorsqu'il en est résulté soit la suppression ou la modification de données contenues dans le système, soit une altération du fonctionnement de ce système, la peine est de trois ans d'emprisonnement et de 100 000 € d'amende.*

*Lorsque les infractions prévues aux deux premiers alinéas ont été commises à l'encontre d'un système de traitement automatisé de données à caractère personnel mis en œuvre par l'Etat, la peine est portée à cinq ans d'emprisonnement et à 150 000 € d'amende".*

[269] En este sentido, SÉDALLIAN, V., "Accès à une base de données mal sécurisée et responsabilités pénales", en *Journaldunet*, 6 de febrero de 2003, consultado el 12 de enero de 2017 en http://www.journaldunet.com/solutions/0302/030206_trib_juridique.shtml, con cita de la Sentencia de la Corte de Apelación de París de fecha 30 de octubre de 2002, asunto Kitetoa, donde se declaraba respecto al acceso o mantenimiento en el sitio que no es confidencial si no hay indicación en contra o barrera para el acceso: "*parties de site, qui ne font, par définition, l'objet d'aucune protection de la part de l'exploitant du site ou de son prestataire de services, devant être réputées non confidentielles à défaut de toute indication contraire et de tout obstacle à l'accès*", Sentencia disponible en http://www.kitetoa.com/Pages/Textes/Les_Dossiers/Tati_versus_Kitetoa/arret-cour-appel.shtml, consultado el 12 de enero de 2017.

De esta forma, en cuanto a la exigencia de medidas de seguridad, la legislación francesa sigue el artículo 2 del Convenio Europeo sobre Cibercriminalidad, aprobado por el Consejo de Europa el 23 de noviembre de 2001 y de la DM 2005/222/JAI que no imponían su vulneración, dejando libertad en este punto a los legisladores nacionales, pero como hemos visto, con su referencia al acceso o mantenimiento fraudulento, amplía la previsión del artículo 3 de la Directiva 2013/40/UE, que sólo se refiere a la "*violación de una medida de seguridad*".

Por último, el mismo artículo 323 también regula en su apartado 3-1 las conductas de facilitar el acceso o mantenimiento[270], similar al artículo 197 *ter* del Código español que veremos en el Capítulo IV; en el apartado 4 establece la participación en un grupo o asociación dirigida a la preparación de estas conductas[271]; el apartado 4-1 se dedica a los supuestos en que se lleva a cabo el acceso en un

---

270 "*Article 323-3-1*

*Le fait, sans motif légitime, notamment de recherche ou de sécurité informatique, d'importer, de détenir, d'offrir, de céder ou de mettre à disposition un équipement, un instrument, un programme informatique ou toute donnée conçus ou spécialement adaptés pour commettre une ou plusieurs des infractions prévues par les articles 323-1 à 323-3 est puni des peines prévues respectivement pour l'infraction elle-même ou pour l'infraction la plus sévèrement réprimée*".

271 "*Article 323-4*

*La participation à un groupement formé ou à une entente établie en vue de la préparation, caractérisée par un ou plusieurs faits matériels, d'une ou de plusieurs des infractions prévues par les articles 323-1 à 323-3-1 est punie des peines prévues pour l'infraction elle-même ou pour l'infraction la plus sévèrement réprimée*".

grupo organizado y contra un sistema de tratamiento automatizado de datos personales aplicado por el Estado[272]; en el apartado 6 está prevista la responsabilidad penal de las denominadas personas morales por estos delitos[273], responsabilidad que en el ámbito español está prevista en el artículo 197 *quinquies* CP, tal y como se expondrán en el Capítulo VI; y en su apartado 7 se regulan los supuestos de tentativa en relación con estos delitos[274] y que por tanto, al igual que otros Códigos que optan por una sección propia para estos delitos, supone la regulación de estos supuestos en la parte especial, a diferencia del Código español, donde se regula la tentativa en la parte general.

Por tanto, el Código francés tiene el mérito de regular los delitos contra los sistemas informáticos con anterioridad incluso al Convenio Europeo sobre Cibercriminalidad y además lo hace en un capítulo propio, lo que favorece su interpretación, si bien en la línea

---

272 "*Article 323-4-1*

*Lorsque les infractions prévues aux articles 323-1 à 323-3-1 ont été commises en bande organisée et à l'encontre d'un système de traitement automatisé de données à caractère personnel mis en œuvre par l'Etat, la peine est portée à dix ans d'emprisonnement et à 300 000 € d'amende*".

273 "*Article 323-6*

*Les personnes morales déclarées responsables pénalement, dans les conditions prévues par l'article 121-2, des infractions définies au présent chapitre encourent, outre l'amende suivant les modalités prévues par l'article 131-38, les peines prévues par l'article 131-39.*

*L'interdiction mentionnée au 2° de l'article 131-39 porte sur l'activité dans l'exercice ou à l'occasion de l'exercice de laquelle l'infraction a été commise*".

274 *"Article 323-7*

*La tentative des délits prévus par les articles 323-1 à 323-3-1 est punie des mêmes peines".*

de otros Códigos que se han expuesto, también los regula junto a otros delitos contra la propiedad, compartiendo el mismo título, con los consiguientes problemas de delimitación del bien jurídico que puede conllevar su ubicación sistemática.

### *4.8 Grecia.*

En el ámbito griego las conductas relacionadas con el *hacking* tienen su regulación penal en el artículo 370Γ, introducido en el año 2001 en su Código de 1951[275], dentro de su libro segundo dedicado a la parte especial y el capítulo vigésimo segundo donde se regula la vulneración de secretos.

Tras establecer en el primer apartado del citado precepto las conductas de copia o uso de programas de ordenador, se disponen en su apartado 2 los supuestos de *hacking* con las penas para el que acceda a datos contenidos en un sistema informático o transmitidos por un sistema de telecomunicaciones, en caso de particular prohibición o vulnerando medidas de seguridad, concluyendo el apartado 3 excluyendo los supuestos en los que el ofensor actúe al

[275] El Código Penal griego de 17 de agosto de 1950, tras la reforma de 2001 se encuentra disponible en http://www.ministryofjustice.gr/site/kodikes/%CE%95%CF%85%CF%81%CE%B5%CF%84%CE%AE%CF%81%CE%B9%CE%BF/%CE%A0%CE%9F%CE%99%CE%9D%CE%99%CE%9A%CE%9F%CE%A3%CE%9A%CE%A9%CE%94%CE%99%CE%9A%CE%91%CE%A3/tabid/432/language/el-GR/Default.aspx, consultado el 12 de enero de 2017.

servicio del legítimo propietario de los datos, salvo que exista expresa prohibición legal o por escrito del propietario[276].

En consecuencia, el Código griego no dedica un capítulo específico para estos delitos, puesto que los regula entre los delitos relativos a la vulneración de secretos, ni incluye un apartado para definiciones como las incluidas en la Directiva 2013/40/UE o la DM 2005/222/JAI, no se refiere al acceso al sistema informático, sino a los datos que contiene, tal y como estaba también previsto en el anterior artículo 197.3 del CP español tras la reforma de la LO 5/2010, ni tampoco regula las conductas de permanencia en el sistema en contra de la voluntad de quien tenga derecho a excluirlo, tal y como incluye el artículo 197 *bis* 1 del Código español, que se analizará en el siguiente Capítulo. Además, en el ámbito griego destaca la ampliación

---

276 El artículo 370Γ establece "*1. Όποιος χωρίς δικαίωμα αντιγράφει ή χρησιμοποιεί προγράμματα υπολογιστών, τιμωρείται με φυλάκιση μέχρι έξι μήνες και με χρηματική ποινή "διακοσίων ενενήντα (290) ΕΥΡΩ [100.000 δρχ.]* έως πέντε χιλιάδων εννιακοσίων (5.900) ΕΥΡΩ" [2.000.000 δρχ.]*.*

*2. Όποιος αποκτά πρόσβαση σε στοιχεία που έχουν εισαχθεί σε υπολογιστή ή σε περιφερειακή μνήμη υπολογιστή ή μεταδίδονται με συστήματα τηλεπικοινωνιών, εφόσον οι πράξεις αυτές έγιναν χωρίς δικαίωμα, ιδίως με παραβίαση απαγορεύσεων ή μέτρων ασφάλειας που είχε λάβει ο νόμιμος κάτοχός τους, τιμωρείται με φυλάκιση μέχρι τρεις μήνες ή με χρηματική ποινή τουλάχιστον "είκοσι εννέα (29) ΕΥΡΩ" [10.000 δρχ.]*. Αν η πράξη αναφέρεται στις διεθνείς σχέσεις ή στην ασφάλεια του κράτους, τιμωρείται κατά το άρθρο 148.*

*3. Αν ο δράστης είναι στην υπηρεσία του νόμιμου κατόχου των στοιχείων, η πράξη της προηγούμενης παραγράφου τιμωρείται μόνο αν απαγορεύεται ρητά από εσωτερικό κανονισμό ή από έγγραφη απόφαση του κατόχου ή αρμόδιου υπαλλήλου του.*

*4. Οι πράξεις των παραγράφων 1 έως 3 διώκονται ύστερα από έγκληση*".

de las previsiones incluidas en el artículo 3 de la Directiva 2013/40/UE, donde se exige expresamente que el acceso "*se haya cometido con violación de una medida de seguridad*", por cuanto comprende en el precepto tanto los supuestos en que se han vulnerado medidas de seguridad como los casos en que existe una prohibición expresa para el acceso a los datos.

### *4.9 Holanda.*

En el ámbito holandés la ratificación del Convenio Europeo sobre Cibercriminalidad fue realizada el 16 de noviembre de 2006.

La regulación de los delitos de *hacking* en el Código penal holandés de 3 de marzo de 1881 fue introducida en su artículo 138a por la Ley de 1 de junio de 2006[277], donde se castigaba como responsable de un delito de intrusión informática al que accediera intencionada e ilegalmente en todo o parte de un sistema automatizado si se ha vulnerado su seguridad, por medios tecnológicos, usando llaves falsas o asumiendo falsa identidad.

Estos delitos se encuentran actualmente en el artículo 138ab[278]

[277] Ley disponible en https://www.eerstekamer.nl/behandeling/20060713/publicatie_wet_2/document3/f=/w26671st.pdf, consultado el 12 de enero de 2017.

[278] El artículo 138ab dispone: "*1 Met gevangenisstraf van ten hoogste een jaar of geldboete van de vierde categorie wordt, als schuldig aan computervredebreuk, gestraft hij die opzettelijk en wederrechtelijk*

del Código, dentro del título V dedicado a los delitos contra el orden público, de su libro segundo que regula los delitos en particular.

El citado precepto regula el acceso intencionado e ilegal a todo o parte de un sistema automatizado, tal y como se encuentra previsto en el artículo 197 *bis* 1 del Código español, si bien en el caso holandés, además, vulnerando las medidas de seguridad, empleando medios tecnológicos, usando llaves falsas o adoptado una falsa identidad, estableciendo mayores penas para el caso de copia de los datos tras el acceso, si se lleva a cabo una intromisión en red pública

---

*binnendringt in een geautomatiseerd werk of in een deel daarvan. Van binnendringen is in ieder geval sprake indien de toegang tot het werk wordt verworven:*

*A door het doorbreken van een beveiliging,*

*B door een technische ingreep,*

*C met behulp van valse signalen of een valse sleutel, of*

*D door het aannemen van een valse hoedanigheid.*

*2 Met gevangenisstraf van ten hoogste vier jaren of geldboete van de vierde categorie wordt gestraft computervredebreuk, indien de dader vervolgens gegevens die zijn opgeslagen, worden verwerkt of overgedragen door middel van het geautomatiseerd werk waarin hij zich wederrechtelijk bevindt, voor zichzelf of een ander overneemt, aftapt of opneemt.*

*3 Met gevangenisstraf van ten hoogste vier jaren of geldboete van de vierde categorie wordt gestraft computervredebreuk gepleegd door tussenkomst van een openbaar telecommunicatienetwerk, indien de dader vervolgens*

*A met het oogmerk zichzelf of een ander wederrechtelijk te bevoordelen gebruik maakt van verwerkingscapaciteit van een geautomatiseerd werk;*

*B door tussenkomst van het geautomatiseerd werk waarin hij is binnengedrongen de toegang verwerft tot het geautomatiseerd werk van een derde".*

Disponible en http://wetten.overheid.nl/BWBR0001854/2014-07-01, consultado en fecha 12 de enero de 2017.

de telecomunicaciones, si hay intención de obtener un beneficio para sí o para un tercero, o si se accede a una tercera computadora.

Una de las peculiaridades del Código holandés es que también se castiga en su artículo 138b[279] al que intencionadamente e ilegalmente impide el acceso o la utilización de un sistema informático ajeno utilizado para proporcionar o transmitir datos.

Por su parte, el artículo 139d, bajo la rúbrica relativa a los recursos técnicos, castiga en su apartado 2 al que con la intención de cometer, entre otros, el delito del artículo 138ab, fabrica, vende, adquiere, importa, distribuye, hace disponible o tiene una herramienta técnica diseñada principalmente para cometer el delito, o bien vende, adquiere, distribuye, hace disponible o tiene en posesión una contraseña de ordenador, código de acceso o datos similares con los que puede ganar el acceso a un dispositivo informatizado o parte del mismo, de forma similar al artículo 197 *ter* del Código español, que veremos en el Capítulo IV. Las penas se incrementan en el apartado 3 cuando el sujeto que cometa el delito previsto en el artículo 139d tenga la intención de cometer el delito del artículo 138ab.

Por último, el Código holandés no regula el supuesto de mantenimiento en el sistema que contiene el artículo 197 *bis* 1 del Código español junto al *hacking*. Sin embargo, tal y como sucede en

---

[279] El artículo 138b establece: "*Met gevangenisstraf van ten hoogste een jaar of geldboete van de vierde categorie wordt gestraft hij die opzettelijk en wederrechtelijk de toegang tot of het gebruik van een geautomatiseerd werk belemmert door daaraan gegevens aan te bieden of toe te zenden*".

el Convenio Europeo sobre Cibercriminalidad, la DM 2005/222/JAI, o la Directiva 2013/40/UE, incluye la definición de datos en su artículo 80 *quinquies*[280] y la definición de computadora en su artículo 80 *sexies*[281], lo que facilita la labor interpretativa de los citados delitos.

### *4.10 Irlanda.*

Aunque en el caso de Irlanda existe una norma penal especial para el intrusismo informático, su referencia se incluye en este epígrafe porque su tipificación se realiza junto a otros delitos de daños en la denominada *Criminal Damage Act* de 1991[282] .

La norma establece en su sección 1 la definición de determinados términos en relación con esta norma, entre los que

---

[280] El artículo 80 *quinquies* establece como definición de datos: "*Onder gegevens wordt verstaan iedere weergave van feiten, begrippen of instructies, op een overeengekomen wijze, geschikt voor overdracht, interpretatie of verwerking door personen of geautomatiseerde werken*", definición similar a la contenida en el artículo 1.b del Convenio Europeo sobre Cibercriminalidad y el artículo 2.b de la Directiva 2013/40/UE.

[281] El artículo 80 *sexies* establece la definición de computadora en los siguientes términos: "*Onder geautomatiseerd werk wordt verstaan een inrichting die bestemd is om langs elektronische weg gegevens op te slaan, te verwerken en over te dragen*", en la misma línea que la definición del artículo 1.a del Convenio Europeo sobre Cibercriminalidad y el artículo 2.a de la Directiva 2013/40/UE.

[282] El Criminal Damage Act de 1991 está disponible en http://www.irishstatutebook.ie/eli/1991/act/31/enacted/en/print#sec5, consultado el 12 de enero de 2017.

incluye los datos. Sigue así el sistema de incluir conceptos establecido en la normativa internacional, ofreciendo el reltativo a los datos, de forma más simplificada que el contemplado en el artículo 1.b) del Convenio Europeo sobre Cibercriminalidad, la definición del artículo 1.b) de la DM 2005/222/JAI y 2.b) de la Directiva 2013/40/UE, regulando en su sección 5 al acceso no autorizado a esos datos. En concreto, esta sección se ocupa de las conductas del que ilegalmente opera en un ordenador irlandés, con intención de acceder a los datos almacenados, comprendiendo tanto los ataques desde el extranjero como los domésticos, distinguiendo la pena en función de que el sujeto acceda o no a los datos y excluyendo los supuestos en los que la persona pretende acceder a datos particulares o conservados por particulares[283].

Por su parte, la sección 6[284] está dedicada a las excusas legales

---

[283] La sección 5 establece: "*Unauthorised accessing of data. 5.—(1) A person who without lawful excuse operates a computer—*

*(a) within the State with intent to access any data kept either within or outside the State, or (b) outside the State with intent to access any data kept within the State, shall, whether or not he accesses any data, be guilty of an offence and shall be liable on summary conviction to a fine not exceeding £500 or imprisonment for a term not exceeding 3 months or both.*

*(2) Subsection (1) applies whether or not the person intended to access any particular data or any particular category of data or data kept by any particular person".*

[284] La sección 6 dispone: "*Without lawful excuse". 6.—(1) This section applies to—*

*(a) any offence under section 2 (1) or 5 , (b) any offence under section 3 other than one involving a threat by the person charged to damage property in a way which he knows is likely to endanger the life of another, and (c) any offence under section 4 other than one involving an*

en relación con los citados comportamientos, con referencia a la consideración de que el sujeto se creía autorizado, o si es la misma persona con derecho a consentir, siendo indiferente si la creencia está justificada o no, si se ha llevado a cabo con honestidad.

---

*intent by the person charged to use, or cause or permit the use of, something in his custody or under his control to damage property in such a way as aforesaid.*

*(2) A person charged with an offence to which this section applies shall, whether or not he would be treated for the purposes of this Act as having a lawful excuse apart from this subsection, be treated for those purposes as having a lawful excuse— (a) if at the time of the act or acts alleged to constitute the offence he believed that the person or persons whom he believed to be entitled to consent to or authorise the damage to (or, in the case of an offence under section 5 , the accessing of) the property in question had consented, or would have consented to or authorised it if he or they had known of the damage or the accessing and its circumstances,*

*(b) in the case of an offence under section 5 , if he is himself the person entitled to consent to or authorise accessing of the data concerned, or (c) if he damaged or threatened to damage the property in question or, in the case of an offence under section 4 , intended to use or cause or permit the use of something to damage it, in order to protect himself or another or property belonging to himself or another or a right or interest in property which was or which he believed to be vested in himself or another and, at the time of the act or acts alleged to constitute the offence, he believed— (i) that he or that other or the property, right or interest was in immediate need of protection, and(ii) that the means of protection adopted or proposed to be adopted were or would be reasonable having regard to all the circumstances.*

*(3) For the purposes of this section it is immaterial whether a belief is justified or not if it is honestly held.*

*(4) For the purposes of subsection (2) a right or interest in property includes any right or privilege in or over land, whether created by grant, licence or otherwise.*

*(5) This section shall not be construed as casting doubt on any defence recognised by law as a defence to criminal charges".*

Por último, la sección 16 de la Ley de abusos informáticos de Reino Unido, de fecha de 29 de junio de 1990, a las que se ha hecho referencia en el epígrafe segundo, tras sus modificaciones por la "*Police and Justice Act 2006*", "*Serious Crime Act 2007*" y el "*Serious Crime Act 2015*", dispone que las menciones a Inglaterra y Gales contenidas en sus secciones 1 (3) (a), 2 (2) (b), 2 (5) (a), 3 (6) (a) y 3A (5) (a), donde se regulan las conductas de *hacking*, también son aplicables en Irlanda del Norte[285].

---

[285] Sección 16. "*Application to Northern Ireland. (1)The following provisions of this section have effect for applying this Act in relation to Northern Ireland with the modifications there mentioned. [F65(1A)In section 1(3)(a)— (a)the reference to England and Wales shall be read as a reference to Northern Ireland; and (b)the reference to 12 months shall be read as a reference to six months.]*
*(2)In section 2(2)(b)—*
*(a)the reference to England and Wales shall be read as a reference to Northern Ireland; and (b)the reference to section 33 of the M4Magistrates' Courts Act 1980 shall be read as a reference to Article 46(4) of the M5Magistrates' Courts (Northern Ireland) Order 1981.*
*[F66(2A)In section 2(5)(a)— (a)the reference to England and Wales shall be read as a reference to Northern Ireland; and (b)the reference to 12 months shall be read as a reference to six months.]*
*(3)F67. . . . . .*
*[F68(3A)In section 3(6)(a)—(a)the reference to England and Wales shall be read as a reference to Northern Ireland; and (b)the reference to 12 months shall be read as a reference to six months.]*
*[F69(3B)In section 3A(5)(a)—(a)the reference to England and Wales shall be read as a reference to Northern Ireland; and (b)the reference to 12 months shall be read as a reference to six months.]*
*(4)[F70Subsection (7) below shall apply in substitution for subsection (3) of section 7]; F71. . . .*
*F72(5). . . . . .*
*F72(6). . . . . .*

*(7)The following paragraphs shall be inserted after Article 3(1) of that Order—"(1A)Subject to section 8 of the Computer Misuse Act 1990 (relevance of external law), if this paragraph applies to an act, what the person doing it had in view shall be treated as an offence to which this Article applies.*

*(1B)Paragraph (1A) above applies to an act if—(a)it is done in Northern Ireland; and (b)it would fall within paragraph (1) as more than merely preparatory to the commission of an offence under section 3 of the Computer Misuse Act 1990 but for the fact that the offence, if completed, would not be an offence triable in Northern Ireland.".*

*(8)In section 8—(a )F72. . . . . (b)the reference in subsection (3) to section 1(1A) of the M6Criminal Attempts Act 1981 shall be read as a reference to Article 3(1A) of that Order.*

*(9)The references in sections 9(1) and 10 to England and Wales shall be read as references to Northern Ireland.*

*[F73(9A)In section 10 the definition of "enactment" shall be read as including a reference to an enactment, whenever passed or made, contained in Northern Ireland legislation or in an instrument made under such legislation.]*

*(10)F74. . . . . .*

*(11)F74. . . . . .*

*(12)F74. . . . . .*

*Amendments (Textual)*

*F65 S. 16(1A) inserted (1.10.2008) by Police and Justice Act 2006 (c. 48), ss. 52, 53, Sch. 14 para. 27(2) (with s. 38(2)); S.I. 2008/2503, art. 2*

*F66 S. 16(2A) inserted (1.10.2008) by Police and Justice Act 2006 (c. 48), ss. 52, 53, Sch. 14 para. 27(3); S.I. 2008/2503, art. 2*

*F67 S. 16(3) repealed (1.10.2008) by Police and Justice Act 2006 (c. 48), ss. 52, 53, Sch. 14 para. 27(4), Sch. 15 Pt. 4 (with s. 38(4)); S.I. 2008/2503, art. 2*

*F68 S. 16(3A) inserted (1.10.2008) by Police and Justice Act 2006 (c. 48), ss. 52, 53, Sch. 14 para. 27(5) (with s. 38(4)); S.I. 2008/2503, art. 2*

*F69 S. 16(3B) inserted (1.10.2008) by Police and Justice Act 2006 (c. 48), ss. 52, 53, Sch. 14 para. 27(6); S.I. 2008/2503, art. 2*

*F70 Words in s. 16(4) substituted (4.9.1998) by 1998 c. 40, s. 9(1), Sch. 1 Pt. II para. 6(3)(a) (with s. 9(3))*

*F71 Words in s. 16(4) repealed (1.10.2008) by Serious Crime Act 2007 (c. 27), ss. 63(1)(2), 92, 94, Sch. 6 para. 59(6), Sch. 14 (with Sch. 13 para. 5); S.I. 2008/2504, art. 2*

Esto es, en Irlanda destaca la existencia de una ley penal especial para regular los delitos de daños en el ámbito irlandés, ofreciendo unos conceptos previos y castigando el acceso a los datos, en lugar de referirlo al sistema informático. Además, la norma no se ocupa de la vulneración de medidas de seguridad para el acceso que se exige en el artículo 3 de la Directiva 2013/40/UE, ni del mantenimiento en el sistema contra la voluntad de quien tenga el legítimo derecho a excluirlo que contempla el artículo 197 *bis* 1 del Código español, pero incluye las citadas excusas absolutorias en su sección 6.

Por todo ello, es significativa la existencia de una norma especial en Irlanda como un posible primer paso para la regulación de las conductas de *hacking* con autonomía propia, incluyendo conceptos y excusas absolutorias en la misma ley. Sin embargo, el hecho de que el legislador irlandés las regule junto a otros delitos de daños sigue impidiendo la plena autonomía sistemática de los delitos informáticos.

---

*F72 S. 16(5)(6)(8)(a) repealed (4.9.1998) by 1998 c. 40, s. 9(1)(2), Sch. 1 Pt. II para. 6(3)(b), Sch. 2 Pt. II (with s. 9(3))*
*F73 S. 16(9A) inserted (3.5.2015) by Serious Crime Act 2015 (c. 9), ss. 44(3), 88(1); S.I. 2015/820, reg. 2(d)*
*F74 S. 16(10)(11)(12) repealed (1.10.2008) by Police and Justice Act 2006 (c. 48), ss. 52, 53, Sch. 14 para. 27(4), Sch. 15 Pt. 4 (with s. 38(2)); S.I. 2008/2503, art. 2".*
Ley disponible en su texto original en http://www.legislation.gov.uk/ukpga/1990/18/pdfs/ukpga_19900018_en.pdf, y con sus reformas en http://www.legislation.gov.uk/ukpga/1990/18, consultado el 26 de enero de 2016.

### *4.11 Italia.*

En el ámbito italiano, al igual que sucediera en Francia[286], con anterioridad a firmar el Convenio Europeo sobre Cibercriminalidad el 23 de noviembre de 2001, el Código penal ya regulaba las conductas de *hacking* en su artículo 615 *ter* como consecuencia de la Ley nº 547 de 23 de diciembre de 1993[287].

Actualmente, el Código penal italiano sigue tipificando estos supuestos en su artículo 615 *ter*[288], bajo la rúbrica relativa al acceso

---

286 *Vid*., *supra* subepígrafe 4.7 de este Capítulo.

287 El artículo 615 *ter* del Código penal italiano fue introducido por el artículo 4 de la Legge, 23 dicembre 1993, n. 547 Modificazioni ed integrazioni alle norme del codice penale e del codice di procedura penale in tema di criminalita' informatica, disponible en http://www.wipo.int/wipolex/es/text.jsp?file_id=230249, consultado el 12 de enero de 2017.

288 "*Accesso abusivo ad un sistema informatico o telematico (1)*
*Chiunque abusivamente si introduce in un sistema informatico o telematico protetto da misure di sicurezza ovvero vi si mantiene contro la volontà espressa o tacita di chi ha il diritto di escluderlo, è punito con la reclusione fino a tre anni.*
*La pena è della reclusione da uno a cinque anni:*
*1) se il fatto è commesso da un pubblico ufficiale o da un incaricato di un pubblico servizio, con abuso dei poteri o con violazione dei doveri inerenti alla funzione o al servizio, o da chi esercita anche abusivamente la professione di investigatore privato, o con abuso della qualità di operatore del sistema;*
*2) se il colpevole per commettere il fatto usa violenza sulle cose o alle persone, ovvero se è palesemente armato;*
*3) se dal fatto deriva la distruzione o il danneggiamento del sistema o l'interruzione totale o parziale del suo funzionamento, ovvero la distruzione o il danneggiamento dei dati, delle informazioni o dei*

abusivo a un sistema informático o telemático, en la sección IV dedicada a los delitos contra la inviolabilidad del domicilio del capítulo III, que contiene los delitos contra la libertad individual, y libro segundo relativo a los delitos en particular.

El citado artículo, con el que tienen claro paralelismo el artículo 197 *bis* 1 y el anterior 197.3 del Código penal español según veremos en el Capítulo IV, comprende tanto las conductas de acceso al sistema informático como la permanencia en el mismo contra la voluntad de quien tenga derecho a excluirlo, requiriendo que el sistema esté protegido con medidas de seguridad, aunque no exige que sean infringidas, siguiendo en este punto lo dispuesto en el artículo 2 del el Convenio Europeo sobre Cibercriminalidad y en la DM 2005/222/JAI, que dejaban libertad a los Estados para decidir si exigían o no que las medidas de seguridad fueran infringidas, pero no sigue lo ordenado en el artículo 3 de la Directiva 2013/40/UE, donde se ordena que en la regulación de estas conductas esté prevista la "*violación de una medida de seguridad*".

---

*programmi in esso contenuti.*
*Qualora i fatti di cui ai commi primo e secondo riguardino sistemi informatici o telematici di interesse militare o relativi all'ordine pubblico o alla sicurezza pubblica o alla sanità o alla protezione civile o comunque di interesse pubblico, la pena è, rispettivamente, della reclusione da uno a cinque anni e da tre a otto anni.*
*Nel caso previsto dal primo comma il delitto è punibile a querela della persona offesa; negli altri casi si procede d'ufficio*". Código Penal de 19 de octubre de 1930, reformado, disponible en http://www.diritto.it/codici/titolo/75-codice-penale-dei-delitti-contro-la-persona, consultado el 12 de enero de 2017.

El mismo precepto regula como agravantes las conductas de *hacking* llevadas a cabo: (i) por un funcionario público o encargado de servicio público, con abuso de poder o con violación de los deberes inherentes a su cargo, o abusivamente por detective privado o con abuso de la cualidad de operador del sistema, abarcando de esta forma un abanico más amplio que las conductas del artículo 198 del CP español, que sólo regula las conductas llevadas a cabo por autoridad o funcionario público según se expondrá en el Capítulo V; (ii) si se lleva a cabo la conducta con violencia; (iii) en el caso de se cause daño o interrupción del sistema, o bien destrucción o corrupción de datos, información o programas que contenga.

El citado artículo 615 *ter* concluye regulando como agravante los casos en que los accesos se refieran a sistemas informáticos o telemáticos de interés militar o relativos al orden o seguridad pública, la salud o la protección civil u otro interés público.

Por último, el artículo 615 *quater*[289] del Código penal italiano,

[289] El artículo 615 *quater* dispone: "*Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici (1)*

*Chiunque, al fine di procurare a sé o ad altri un profitto o di arrecare ad altri un danno, abusivamente si procura, riproduce, diffonde, comunica o consegna codici, parole chiave o altri mezzi idonei all'accesso ad un sistema informatico o telematico, protetto da misure di sicurezza, o comunque fornisce indicazioni o istruzioni idonee al predetto scopo, è punito con la reclusione sino ad un anno e con la multa sino a euro 5.164.*

*La pena è della reclusione da uno a due anni e della multa da euro 5.164 a euro 10.329 se ricorre taluna delle circostanze di cui ai numeri 1 e 2 del quarto comma dell'articolo 617quater*", disponible en http://www.diritto.it/codici/articolo/4304202-codice-penale-detenzione-e-

bajo la rúbrica relativa a la posesión ilegal y la circulación de códigos de acceso a sistemas informáticos o telemáticos, castiga al que con el fin de obtener para sí o para otros un beneficio o causar daño, se procure ilegalmente, reproduzca, difunda, comunique o entregue códigos, contraseñas u otros medios de acceso a un sistema informático o telemático, protegido por medidas de seguridad o comunique indicaciones o instrucciones idóneas para este propósito. Por tanto, el precepto es similar al artículo 197 *ter* del Código español aunque en el caso español no se requiere esa finalidad, incrementando las penas si se causa perjuicio a un sistema informático o telemático utilizado por el Estado u otro ente público o empresa que presta servicio público o de utilidad pública, o bien se lleva a cabo la conducta por funcionario público o persona encargada de servicio público, cuando la realiza con abuso de poder o violación de las obligaciones inherentes a su cargo o mediante abuso de su función de gestor de red.

En conclusión, aunque como en la mayoría de países de nuestro entorno en el ámbito italiano tampoco existe una regulación autónoma de los delitos informáticos, destaca que la regulación de estas conductas estuviese tipificada en el Código penal con anterioridad al Convenio Europeo de Cibercriminalidad y, además, su ubicación entre los delitos contra la inviolabilidad del domicilio, planteando el debate sobre la inviolabilidad del domicilio informático

diffusione-abusiva-di-codici-di-accesso-a-sistemi-informatici-o-telematici, consultado el 23 de septiembre de 2016.

como bien jurídico protegido en los delitos de *hacking*, cuestión a la que se hará referencia en el Capítulo siguiente.

### *4.12 Letonia.*

El Código penal letón de 17 de junio de 1998[290] dedica el capítulo XX de su parte especial a los delitos contra la seguridad general y el orden público. Entre estos delitos se encuentran las conductas de acceso arbitrario a sistemas de procesamiento automatizado de datos en su sección 241, introducida por la Ley de 28 de abril de 2005[291] y modificado por la Ley de 25 de septiembre de 2014[292].

El citado precepto establece en su primer apartado la pena para las personas que sin la debida autorización accedan a un sistema de tratamiento automatizado de datos o a parte del mismo, vulnerando los sistemas de protección o si causan un daño sustancial en ellos, incrementando las penas en su apartado segundo para los supuestos en los que el sujeto tiene un propósito de adquirir la propiedad, y estableciendo en su apartado tercero mayores penas en los casos en

290 El Código Penal letón de 1998, con sus reformas, se encuentra disponible en http://likumi.lv/doc.php?id=88966, donde también se incluye su versión en inglés, consultado el 12 de enero de 2017.

291 Ley disponible en http://likumi.lv/doc.php?id=108357, consultado el 12 de enero de 2017.

292 Ley disponible en http://likumi.lv/ta/id/269516-grozijumi-kriminallikuma, consultado el 12 de enero de 2017.

que se causan graves consecuencias o si las conductas se dirigen contra un sistema de tratamiento automatizado de datos que procesa información relacionada con la política, economía, ejército u otras garantías sociales del país[293].

[293] La sección 241 establece: *"241.pants. Patvaļīga piekļūšana automatizētai datu apstrādes sistēmai. (1) Par patvaļīgu piekļūšanu automatizētas datu apstrādes sistēmas resursiem, ja tas saistīts ar sistēmas aizsardzības līdzekļu pārvarēšanu vai ja tas izdarīts bez attiecīgas atļaujas vai izmantojot citai personai piešķirtas tiesības un ja ar to radīts būtisks kaitējums, — soda ar brīvības atņemšanu uz laiku līdz diviem gadiem vai ar īslaicīgu brīvības atņemšanu, vai ar piespiedu darbu, vai ar naudas sodu. (2) Par šā panta pirmajā daļā paredzēto noziedzīgo nodarījumu, ja tas izdarīts mantkārīgā nolūkā, — soda ar brīvības atņemšanu uz laiku līdz četriem gadiem vai ar īslaicīgu brīvības atņemšanu, vai ar piespiedu darbu, vai ar naudas sodu, konfiscējot mantu vai bez mantas konfiskācijas. (3) Par šā panta pirmajā daļā paredzētajām darbībām, ja tās izraisījušas smagas sekas vai ja tās vērstas pret automatizētu datu apstrādes sistēmu, kas apstrādā informāciju, kura saistīta ar valsts politisko, ekonomisko, militāro, sociālo vai citu drošību, — soda ar brīvības atņemšanu uz laiku līdz pieciem gadiem vai ar īslaicīgu brīvības atņemšanu, vai ar piespiedu darbu, vai ar naudas sodu, konfiscējot mantu vai bez mantas konfiskācijas".* Y en su versión en inglés: "*Section 241. Arbitrary Accessing Automated Data Processing Systems. (1) For a person who commits arbitrary accessing an automated data processing system, if it is related to breaching of system protective means or if it is carried out without the relevant permission or using the rights granted to another person, and if substantial harm has been caused thereby, the applicable punishment is deprivation of liberty for a term up to two years or temporary deprivation of liberty, or community service, or a fine. (2) For the criminal offence provided for in Paragraph one of this Section, if it has been committed for purposes of acquiring property, the applicable punishment is deprivation of liberty for a term up to four years or temporary deprivation of liberty, or community service, or a fine, with or without confiscation of property. (3) For the acts provided for in Paragraph one of this Section, if serious consequences have been caused thereby, or if they are directed against automated data processing systems that process*

Por otro lado, su artículo 244[294] castiga al que lleve a cabo la fabricación ilegal, adaptación para su utilización, venta, distribución o almacenamiento de herramientas (dispositivos, software, contraseña de ordenador, código de acceso o datos similares), destinados a influir en los recursos de un sistema automatizado o con la ayuda de los

---

*information related to State political, economic, military, social or other security, the applicable punishment is deprivation of liberty for a term up to five years or temporary deprivation of liberty, or community service, or a fine, with or without confiscation of property".*

[294] El artículo 244 del Código Penal letón establece: "*244.pants. Nelikumīgas darbības ar automatizētas datu apstrādes sistēmas resursu ietekmēšanas ierīcēm (1) Par tāda rīka (ierīces, datorprogrammas, datorparoles, pieejas koda vai līdzīgu datu) neatļautu izgatavošanu, pielāgošanu izmantošanai, realizēšanu, izplatīšanu vai glabāšanu, kurš paredzēts automatizētas datu apstrādes sistēmas resursu ietekmēšanai vai ar kura palīdzību var piekļūt automatizētas datu apstrādes sistēmai vai tās daļai nolūkā izdarīt noziedzīgu nodarījumu, — soda ar brīvības atņemšanu uz laiku līdz diviem gadiem vai ar īslaicīgu brīvības atņemšanu, vai ar piespiedu darbu, vai ar naudas sodu. (2) Par tādām pašām darbībām, ja tās izraisījušas smagas sekas, — soda ar brīvības atņemšanu uz laiku līdz pieciem gadiem vai ar īslaicīgu brīvības atņemšanu, vai ar piespiedu darbu, vai ar naudas sodu".*

En su versión en inglés: "*Section 244. Illegal Operations with Automated Data Processing System Resource Influencing Devices. (1) For a person who commits the illegal manufacture, adaptation for utilisation, sale, distribution or storage of such tool (device, software, computer password, access code or similar data), which is intended for the influencing of resources of an automated data processing system or with the aid of which access to an automated data processing system or a part thereof is possible for purposes of committing a criminal offence, the applicable punishment is deprivation of liberty for a term up to two years or temporary deprivation of liberty, or community service, or a fine. (2) For a person who commits the same acts, if serious consequences has been caused thereby, the applicable punishment is deprivation of liberty for a term up to five years or temporary deprivation of liberty, or community service, or a fine".*

cuales se acceda a un sistema de tratamiento automatizado de datos o parte del mismo, similar al delito del artículo 197 *ter* del Código español que se expondrá en el Capítulo IV, incrementando las penas en su apartado segundo para el caso de que se existan consecuencias graves causadas por estos hechos.

Por tanto, en el ámbito letón se regula el acceso a sistemas de tratamiento automatizado de datos, con vulneración de medidas de seguridad, en la misma línea que exige el artículo 3 de la Directiva 2013/40/UE, pero sin incluir los conceptos previos que define la Directiva ni tampoco la regulación expresa de las conductas de mantenimiento en el sistema que incluye el Código español. Aunque el Código letón no dedica un capítulo propio a los delitos informáticos, es destacable que la regulación del *hacking* se incluya entre los delitos contra la seguridad y el orden público, rúbrica que parece más cercana al bien jurídico protegido por estos delitos, según se expondrá en el siguiente Capítulo.

### *4.13 Lituania.*

El Código penal lituano, de 26 de septiembre de 2000[295], regula las conductas de *hacking* en su artículo 198-1, dentro del

[295] Código penal disponible, con sus reformas, en http://www.infolex.lt/portal/start_ta.asp?act=doc&fr=pop&doc=66150, consultado el 12 de enero de 2017.

Capítulo XXX relativo a los delitos contra la seguridad de los datos electrónicos y sistemas de información, introducido por la reforma del Código penal de 2004 y modificado con las reformas de los años 2007 y 2015.

En su redacción originaria de 2004 el precepto regulaba las conductas de acceso ilícito a un sistema informático o red informática con vulneración de las medidas de seguridad establecidas, incluyendo la responsabilidad de las personas jurídicas[296].

Estos supuestos fueron ampliados con la modificación de 2007[297], refiriendo el acceso al sistema de información con violación

---

[296] La redacción inicial del artículo 198-1 tras la reforma por la Ley 29 de enero de 2004 disponía: "*1. Tas, kas neteisėtai prisijungė prie kompiuterio ar kompiuterinio tinklo pažeisdamas kompiuterio ar kompiuterinio tinklo apsaugos priemones, baudžiamas viešaisiais darbais arba bauda, arba areštu, arba laisvės atėmimu iki vienerių metų.*
*2. Už šiame straipsnyje numatytą veiką atsako ir juridinis asmuo*", disponible en http://www3.lrs.lt/pls/inter3/oldsearch.preps2?a=226955&b=, consultado el 12 de enero de 2017.

[297] La reforma de 28 de junio de 2007 establecía la siguiente redacción del artículo 198-1 del Código penal lituano: "*1. Tas, kas neteisėtai prisijungė prie informacinės sistemos pažeisdamas informacinės sistemos apsaugos priemones, baudžiamas viešaisiais darbais arba bauda, arba areštu, arba laisvės atėmimu iki vienerių metų.*
*2. Tas, kas neteisėtai prisijungė prie strateginę reikšmę nacionaliniam saugumui arba didelę reikšmę valstybės valdymui, ūkiui ar finansų sistemai turinčios informacinės sistemos, baudžiamas bauda arba areštu, arba laisvės atėmimu iki trejų metų.*
*3. Už šiame straipsnyje numatytas veikas atsako ir juridinis asmuo*.", reforma disponible en http://www3.lrs.lt/pls/inter3/oldsearch.preps2?a=301997&b=, consultado el 12 de enero de 2017.

de las medidas de seguridad, y estableciendo como novedad mayores penas para los casos en los que se trate de sistemas de información de importancia estratégica para la seguridad nacional o de gran importancia para el gobierno, la economía o el sistema financiero, contemplando igualmente la responsabilidad de las personas jurídicas por estos delitos, y de nuevo fueron ampliados tras la reforma de 2015[298], donde se incluye el mismo acceso pero referido a todo o parte del sistema de información, así como la agravante, ampliada también en el caso de acceso a todo o parte del sistema financiero, siguiendo en ambos casos lo dispuesto en el artículo 2 del Convenio Europeo sobre Cibercriminalidad y de la DM 2005/222/JAI, y se anticipa a las previsiones posteriores del artículo 3 de la Directiva 2013/40/UE relativas al acceso al sistema de información con violación de una medida de seguridad. No obstante, el Código penal lituano no incluye las conductas de mantenimiento en el sistema informático o facilitar el acceso que regula el artículo 197 *bis* 1 del Código penal español.

---

[298] La regulación de estas conductas, tras la reforma del 11 de junio de 2015, establece en el artículo 198-1: "*1. Tas, kas neteisėtai prisijungė prie informacinės sistemos ar jos dalies pažeisdamas informacinės sistemos apsaugos priemones, baudžiamas viešaisiais darbais arba bauda, arba areštu, arba laisvės atėmimu iki dvejų metų.*

*2. Tas, kas neteisėtai prisijungė prie strateginę reikšmę nacionaliniam saugumui ar didelę reikšmę valstybės valdymui, ūkiui ar finansų sistemai turinčios informacinės sistemos ar jos dalies, baudžiamas bauda arba areštu, arba laisvės atėmimu iki trejų metų.*

*3. Už šiame straipsnyje numatytas veikas atsako ir juridinis asmuo*".

Esta reforma está disponible en http://www3.lrs.lt/pls/inter3/oldsearch.preps2?a=1041675&b=, consultado el 12 de enero de 2017.

Por último, su artículo 198-2 castiga al que con fines delictivos o de forma ilegal produzca, transporte, importe, venda, facilite el acceso o de otro modo distribuya o adquiera dispositivos o *software* directamente para cometer estos delitos, así como *passwords*, códigos u otros datos similares para acceder al sistema de información o parte del mismo, de forma similar al artículo 197 *ter* del Código español que veremos en el Capítulo IV, si bien estableciendo también en el mismo precepto la previsión de que estas conductas sean cometidas por una persona jurídica.

Es destacable que, al igual que en el caso de Letonia, se haya incluido el delito de *hacking* en un capítulo junto a otros delitos contra la seguridad de los datos electrónicos y los sistemas de información, dotándole de una cierta autonomía que resulta acorde con el que parece el bien jurídico protegido por estos delitos, según se verá en el siguiente Capítulo.

### *4.14 Luxemburgo.*

En el ámbito de Luxemburgo, su Código penal[299] dedica el libro segundo a los delitos y penas en particular, entre los cuales el título IX regula los delitos contra la propiedad y, dentro de estos

[299] El Código Penal de Luxemburgo de 16 de junio de 1879 se encuentra disponible en http://www.legilux.public.lu/leg/textescoordonnes/codes/code_penal/codepenal.pdf, consultado el 12 de enero de 2017.

supuestos, el capítulo II castiga los fraudes, estableciendo su sección VII.1 ciertos delitos informáticos tras la reforma introducida con la Ley de 15 de julio de 1993[300]. Esta Ley introducía en el artículo 509.1 del Código las penas para la persona que fraudulentamente accede o se mantiene en un sistema de tratamiento o transmisión automática de datos, incrementándose las penas en los supuestos en que se hayan suprimido o modificado datos en el sistema o se hubiese alterado el funcionamiento del sistema, modificándose las cuantías de las multas para incluir la referencia a euros e incluyendo también el acceso o mantenimiento en sistemas de transmisión de automatizada de datos tras la reforma llevada a cabo por la Ley de 14 de agosto de 2000[301].

Por su parte, el artículo 509.3, tras la misma reforma de 1993, regula las conductas del que intencionadamente y sin respetar los derechos de otros, directa o indirectamente se introduzca dentro de un sistema de tratamiento automatizado de datos, o bien suprima o altere esos datos.

---

300 Ley de 15 de julio de 1993 disponible en http://www.legilux.public.lu/rgl/1993/A/1152/1.pdf, consultado el 12 de enero de 2017.

301 El artículo 509.1, tras la reforma de la Ley de 14 de agosto de 2000 establece:"*Quiconque, frauduleusement, aura accédé ou se sera maintenu dans tout ou partie d'un système de traitement ou de transmission automatisé de données sera puni d'un emprisonnement de deux mois à deux ans et d'une amende de 500 euros à 25.000 euros ou de l'une de ces deux peines.*
*Lorsqu'il en sera résulté soit la suppression ou la modification de données contenues dans le système, soit une altération du fonctionnement de ce système, l'emprisonnement sera de quatre mois à deux ans et l'amende de 1.250 euros à 25.000 euros*.".

Con la Ley de 18 de julio de 2014 se introduce en el mismo precepto la interceptación de datos de transmisiones no públicas desde o dentro de un sistema de procesamiento o transmisión automatizada de datos, intencionadamente y en violación de los derechos de los demás[302].

El artículo 509.4 establece como agravante de los citados supuestos aquellos casos en los que ha habido transferencia de dinero o valor monetario, con pérdida de la propiedad a un tercero y con el propósito de obtener una ventaja económica la persona que comete el delito o un tercero[303].

---

302 Tras la reforma de la Ley de 14 de agosto de 2000, el artículo 509.3 también incluye la referencia al acceso a un sistema de transmisión automatizada de datos: "*Quiconque aura, intentionnellement et au mépris des droits d'autrui, directement ou indirectement, introduit des données dans un système de traitement ou de transmission automatisé ou supprimé ou modifié les données qu'il contient ou leurs modes de traitement ou de transmission, sera puni d'un emprisonnement de trois mois à trois ans et d'une amende de 1.250 euros à 12.500 euros ou de l'une de ces deux peines.*", y tras la reforma llevada a cabo por la Ley de 18 de julio de 2014 se incluye un nuevo párrafo a continuación: *"Sera puni des mêmes peines celui qui aura intentionnellement et au mépris des droits d'autrui, intercepté des données lors de transmissions non publiques à destination, en provenance ou à l'intérieur d'un système de traitement ou de transmission automatisé de données*.". La Ley de 18 de julio de 2014 está disponible en http://www.legilux.public.lu/leg/a/archives/2014/0133/a133.pdf, consultado el 12 de enero de 2017.

303 Tras la reforma de 10 de noviembre de 2006, disponible en http://www.legilux.public.lu/rgl/2006/A/3426/A.pdf, consultado el 12 de enero de 2017, el artículo 509.4 establece: "*Lorsque dans les cas visés aux articles 509-1 à 509-3, il y a eu transfert d'argent ou de valeur monétaire, causant ainsi une perte de propriété à un tiers dans un but de procurer un avantage économique à la personne qui ommet l'infraction ou à une tierce*

También está prevista como agravante en el artículo 509.5 la conducta de quien con la intención de defraudar, produjese, vendiese, obtuviese, importaran, distribuyese o pusiere a disposición un dispositivo informático para cometer cualquiera de los delitos del artículo 509.1 a 509.4, o una llave electrónica de acceso a todo o parte de un sistema de procesamiento o transmisión automatizada de datos[304], similar a las conductas tipificadas en el artículo 197 *ter* del Código español, que se expondrá en el Capítulo IV.

Por último, el artículo 509.6 castiga la tentativa en cualquiera de los delitos previstos en los artículos 509.1 a 509.5, llevando así a su parte especial los supuestos que en el Código español se regulan en la parte general, y el artículo 509.7 establece las penas para el que haya

---

*personne, la peine encourue sera un emprisonnement de quatre mois à cinq ans et une amende de 1.250 euros à 30.000 euros.*". Esta reforma también incluía en el precepto las conductas de fabricar, recibir, detener, obtener, vender o transferir un *software* diseñado para la comisión del delito del párrafo anterior: "*Encourront les mêmes peines, ceux qui auront fabriqué, reçu, obtenu, détenu, vendu ou cédé à un tiers des logiciels ayant pour objet de rendre possible une infraction visée à l'alinéa qui précède*", este segundo párrafo del artículo 509.4 fue suprimido por la Ley de 18 de julio de 2014.

[304] El artículo 509.5 fue modificado la Ley de 18 de julio de 2014 derogando la referencia a las conductas de uso de documentos informáticos que se había introducido por la Ley de 15 de julio de 1993 e introduciendo desde el 2014 la agravante aplicable para los supuestos de los artículos 509.1. a 509.4: "*Sera puni de 4 mois à cinq ans d'emprisonnement et d'une amende de 1.250 euros à 30.000 euros quiconque aura, dans une intention frauduleuse, produit, vendu, obtenu, détenu, importé, diffusé ou mis à disposition, – un dispositif informatique destiné à commettre l'une des infractions visées aux articles 509-1 à 509-4; ou – toute clef électronique permettant d'accéder, au mépris des droits d'autrui, à tout ou à partie d'un système de traitement ou de transmission automatisé de données*.".

participado en una asociación formada, también previsto en el artículo 197 *quater* del Código español según se verá en el Capítulo V, o en un acuerdo establecido para la preparación de los citados delitos[305].

Por tanto, el Código de Luxemburgo sigue la línea expuesta de otros países europeos que optan por incluir estos delitos como un delito contra la propiedad, sin establecer un capítulo propio para los delitos informáticos, con los consiguientes problemas que la interpretación sistemática de estas conductas puede llevar en la práctica.

### *4.15 Malta.*

El Código Penal de Malta, de 10 de junio de 1854[306], contiene en su parte II, delitos y penas, el título IX dedicado a los delitos contra la propiedad y la seguridad pública, donde se ubica el subtítulo V relativo a los abusos informáticos, añadido con la reforma de 27 de

[305] Tras la Ley de 15 de julio de 1993, los artículos 509.6 y 509.7 establecen, respectivamente, "*La tentative des délits prévus par les articles 509-1 à 509-5 est punie des mêmes peines que le délit lui-même*" y "*Quiconque aura participé à une association formée ou à une entente établie en vue de la préparation, concrétisée par un ou plusieurs faits matériels, d'une ou de plusieurs infractions prévues par les articles 509-1 à 509-5 sera puni des peines prévues pour l'infraction ellemême ou pour l'infraction la plus sévèrement réprimée*.".

[306] Código Penal de Malta disponible en http://www.justiceservices.gov.mt/DownloadDocument.aspx?app=lom&itemid=8574, consultado el 12 de enero de 2017.

marzo de 2001.

Entre ellos, el artículo 337B incluye las definiciones de ordenador, datos informáticos, red informática, *software* o sistema informático, entre otras[307], y el artículo 337C regula exhaustivamente

[307] *"337B. Interpretation. Added by: III. 2001.27. Amended by: VII. 2010.26; VII. 2010.25; VIII. 2015.23.*
*(1) For the purposes of this Sub-title the following definitions, unless the context otherwise requires, shall apply: "computer" means an electronic device that performs logical, arithmetic and memory functions by manipulating electronic or magnetic impulses, and includes all input, output, processing, storage, software and communication facilities that are connected or related to a computer in a computer system or computer network;*
*"computer data" means any representation of facts, information or concepts in a form suitable for processing in an information system or in a computer system, including a program suitable to cause a computer system to perform a function;*
*"computer network" means the interconnection of communication lines and circuits with a computer through a remote device or a complex consisting of two or more interconnected computers;*
*"computer output" or "output" means a statement or a representation of data whether in written, printed, pictorial, screen display, photographic or other film, graphical, acoustic or other form produced by a computer;*
*"computer software" or "software" means a computer program, procedure or associated documentation used in the operation of a computer system; tape, disk packs, diskettes, CD-roms, computer output, including paper and microform and any storage media, electronic or otherwise;*
*"computer system" means a set of related computer equipment, hardware or software;*
*"function" includes logic, control, arithmetic, deletion, storage, retrieval and communication of data or telecommunication to, from or within a computer;*
*"information system" means a device or group of inter-connected or related devices, one or more of which, pursuant to a programme, automatically processes computer data, as well as computer data stored, processed,*

el acceso ilícito a la información, castigando al que sin autorización utilice un ordenador o cualquier otro dispositivo para acceder a datos, *software* o documentación de apoyo contenida en el equipo, o utilice, copie o modifique cualquiera de esos datos, *software* o documentación; les dé salida, impida o dificulte el acceso, dificulte el funcionamiento u operación de un sistema informático, *software* o la integridad o fiabilidad de los datos; impida o interrumpa el funcionamiento de un sistema informático mediante la introducción de datos en el ordenador, transmitiendo, dañando, borrando, deteriorando, alterando o suprimiendo esos datos o haciéndolos inaccesibles; tome posesión o haga uso de cualquier dato, *software* o documentación de apoyo; instale, mueva, altere, dañe, elimine, deteriore, suprima, destruya, varíe o añada a cualquier dato, *software* o documentación de apoyo; revele una contraseña o cualquier otro medio de acceso, código de acceso u otra información de acceso a cualquier persona no autorizada; use la clave de acceso de otra persona, contraseña de usuario nombre, dirección de correo electrónico u otros medios de acceso o información de identificación en un ordenador o en cualquier forma viole alguna medida de seguridad para obtener acceso sin autorización a la totalidad o a cualquier parte de un sistema informático; revele cualquier información, *software* o soporte documental a menos que sea

---

*retrieved or transmitted by that device or group of devices for the purposes of its or their operation, use, protection and maintenance;*
*"supporting documentation" means any documentation used in the computer system in the construction, clarification, implementation, use or modification of the software or data*".

necesario en el curso de sus funciones o por cualquier otra ley; intercepte por medios técnicos, transmisiones de datos no públicas, hacia, desde o dentro de un sistema de información o sistema informático, incluyendo emisiones electromagnéticas de un sistema de información o un sistema informático que lleve tales datos informáticos; produzca, venda, procure los procedimientos para el uso, importe, distribuya, posea o ponga a disposición un dispositivo, incluyendo un programa de ordenador, diseñado o adaptado principalmente con el propósito de cometer cualquiera de los actos o una contraseña, código de acceso o datos similares por los cuales sea accesible la totalidad o una parte de un sistema de información[308], de

[308] *"337C. Unlawful access to, or use of, information. Added by: III. 2001.27. Amended by: VII. 2010.26; VIII. 2015.24*
*(1) A person who without authorisation does any of the following acts shall be guilty of an offence against this article - (a) uses a computer or any other device or equipment to access any data, software or supporting documentation held in that computer or on any other computer, or uses, copies or modifies any such data, software or supporting documentation;*
*(b) outputs any data, software or supporting documentation from the computer in which it is held, whether by having it displayed or in any other manner whatsoever;*
*(c) copies any data, software or supporting documentation to any storage medium other than that in which it is held or to a different location in the storage medium in which it is held;*
*(d) prevents or hinders access to any data, software or supporting documentation;*
*(e) hinders or impairs the functioning or operation of a computer system, software or the integrity or reliability of any data;*
*(ee) hinders or interrupts the functioning of an information system by inputting computer data, by transmitting, damaging, deleting, deteriorating, altering or suppressing such data, or by rendering such data inaccessible;*

*(f) takes possession of or makes use of any data, software or supporting documentation;*
*(g) installs, moves, alters, damages, deletes, deteriorates, suppresses, destroys, varies or adds to any data, software or supporting documentation or renders such data inaccessible;*
*(h) discloses a password or any other means of access, access code or other access information to any unauthorised person;*
*(i) uses another person's access code, password, user name, electronic mail address or other means of access or identification information in a computer or in any manner infringes any security measure to gain access without authorization to the whole or to any part of an information system;*
*(j) discloses any data, software or supporting documentation unless this is required in the course of his duties or by any other law;*
*(k) intercepts by technical means, non-public transmissions of data, to, from or within an information system or a computer system, including electromagnetic emissions from an information system or a computer system carrying such computer data;*
*(l) produces, sells, procures for use, imports, distributes, possesses or otherwise makes available a device, including a computer program, designed or adapted primarily for the purpose of committing any of the acts in paragraphs (a) to (j) or a computer password, access code, or similar data by which the whole or any part of an information system is capable of being accessed.*
*(2) For the purposes of this Sub-title: (a) a person shall be deemed to act without authorization if he is not duly authorised by an entitled person;*
*(b) a person shall be deemed to be an entitled person if the person himself is entitled to control the activities defined in subarticle (1)(a) to (j) or in article 4(a) and (b) of this Sub-title.*
*(3) For the purposes of subarticle (1): (a) a person shall be deemed to have committed an offence irrespective of whether in the case of any modification, such modification is intended to be permanent or temporary;*
*(b) the form in which any software or data is output and in particular whether or not it represents a form in which, in the case of software, it is capable of being executed or, in the case of data, it is capable of being processed by a computer, is immaterial.*
*(4) For the purposes of subarticle (1)(f), a person who for the fact that he has in his custody or under his control any data, computer software or supporting documentation which he is not authorised to have, shall be*

forma similar por tanto en este último supuesto a la previsión del artículo 197 *ter* del Código español, que será expuesto en el Capítulo IV.

Por último, el artículo 337.f establece las penas correspondientes a las citadas conductas.

Por tanto, el Código maltés incluye una lista de definiciones y contiene una amplia descripción de las conductas relativas al *hacking*, en línea con el sistema seguido en el Convenio Europeo sobre Cibercriminalidad, la DM 2005/222/JAI y la Directiva 2013/40/UE. Aunque las conductas de *hacking* se ubican en un título dedicado a los delitos contra la propiedad, en la línea ya comentada de otros países europeos, destaca que el legislador establezca un subtítulo propio para estos delitos informáticos y lo realice con una minuciosa y extensa regulación del acceso ilícito a datos, *software* o documentación contenida en un equipo informático.

### *4.16 Polonia.*

Tras la reforma llevada a cabo por el Acta de 24 de octubre de 2008[309], el Código penal polaco de 6 de junio de 1997[310] tipifica el

---

*deemed to have taken possession of it*.".

[309] Reforma disponible en http://isip.sejm.gov.pl/Download;jsessionid=FB60783149CC47AA518F60891929BACE?id=WDU20082141344&type=1, consultado el 12 de enero de

acceso a los sistemas de información en su artículo 267[311], dentro del capítulo XXXIII dedicado a los delitos contra la información protegida, castigando al que sin autorización accede a una información protegida no destinada a él, imponiendo iguales penas al que accede sin autorización a todo o parte del sistema de información, así como al que con el fin de obtener una información de la que no es titular, utiliza un dispositivo de espionaje u otro dispositivo o *software*, imponiendo iguales penas al que consiga esta información obtenida con el dispositivo.

Por último, según concluye el citado precepto, estos delitos

---

2017.

310 Código Penal disponible en http://isap.sejm.gov.pl/DetailsServlet?id=WDU19970880553, consultado el 12 de enero de 2017.

311 El artículo 267 establece: "*CZĘŚĆ SZCZEGÓLNA*

*Rozdział XXXIII*

*Przestępstwa przeciwko ochronie informacji*

*Art. 267.*

*§ 1. Kto bez uprawnienia uzyskuje dostęp do informacji dla niego nieprzeznaczonej, otwierając zamknięte pismo, podłączając się do sieci telekomunikacyjnej lub przełamując albo omijając elektroniczne, magnetyczne, informatyczne lub inne szczególne jej zabezpieczenie, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2.*

*§ 2. Tej samej karze podlega, kto bez uprawnienia uzyskuje dostęp do całości lub części systemu informatycznego.*

*§ 3. Tej samej karze podlega, kto w celu uzyskania informacji, do której nie jest uprawniony, zakłada lub posługuje się urządzeniem podsłuchowym, wizualnym albo innym urządzeniem lub oprogramowaniem.*

*§ 4. Tej samej karze podlega, kto informację uzyskaną w sposób określony w § 1–3 ujawnia innej osobie.*

*§ 5. Ściganie przestępstwa określonego w § 1–4 następuje na wniosek pokrzywdzonego".*

sólo son perseguidos a instancia de la víctima.

Es decir, el Código polaco dedica un capítulo a los delitos contra la información protegida y tipifica entre ellos las conductas de *hacking*, dotándole de cierta autonomía respecto a otros delitos que tutelan bienes jurídicos distintos, pero no exige la vulneración de medidas de seguridad en el acceso al sistema de información, no distingue el acceso total o parcial al que se refiere el Convenio Europeo sobre Cibercriminalidad, la DM 2005/222/JAI y la Directiva 2013/40/UE, ni tampoco incluye junto al acceso las conductas de permanencia no autorizada en el sistema que tipifica el artículo 197 *bis* 1 del Código penal español que veremos en el Capítulo IV.

### *4.17 República Checa.*

El Código penal checo de 29 de noviembre de 1961[312] dedicaba en su capítulo nueve (delitos contra la propiedad) el artículo 257.a[313] a los daños o abuso de datos en soportes de grabación. El

[312] Disponible en http://business.center.cz/business/pravo/zakony/trestni_zakon/, consultado el 12 de enero de 2017.

[313] El artículo 257.a disponía: "*§ 257a Poškození a zneužití záznamu na nosiči informací*

*(1) Kdo získá přístup k nosiči informací a v úmyslu způsobit jinému škodu nebo jinou újmu nebo získat sobě nebo jinému neoprávněný prospěch*

*a) takových informací neoprávněně užije,*

*b) informace zničí, poškodí, změní nebo učiní neupotřebitelnými, nebo*

precepto fue introducido por la Ley 557/1991 y castigaba en su primer apartado al sujeto que con intención de causar daños o algún otro perjuicio ajeno, u obtener un beneficio injusto para sí o para un tercero, accediera a un soporte de datos y realizara alguna de las conductas que describía: (i) utilizar esos datos sin autorización; (ii) destruir, dañar o inutilizar los datos; (iii) interferir con el *hardware* o *software* de un ordenador.

Las penas se agravaban en el segundo apartado en el caso de que los hechos se cometieran como miembro de un grupo organizado o si se causaba un daño sustancial o se obtenía un beneficio sustancial para sí o para un tercero.

Por último, el precepto castigaba con mayores penas al sujeto que causara daños a gran escala o adquiriera beneficios a gran escala para sí o para un tercero.

Tras la Ley de 8 de enero de 2009, que aprueba el nuevo

---

*c) učiní zásah do technického nebo programového vybavení počítače nebo jiného telekomunikačního zařízení,*
*bude potrestán odnětím svobody až na jeden rok nebo zákazem činnosti nebo peněžitým trestem nebo propadnutím věci nebo jiné majetkové hodnoty.*

*(2) Odnětím svobody na šest měsíců až tři léta bude pachatel potrestán,*

*a) spáchá-li čin uvedený v odstavci 1 jako člen organizované skupiny, nebo*

*b) způsobí-li takovým činem značnou škodu nebo získá-li sobě nebo jinému značný prospěch.*

*(3) Odnětím svobody na jeden rok až pět let bude pachatel potrestán, způsobí-li činem uvedeným v odstavci 1 škodu velkého rozsahu nebo získá-li sobě nebo jinému prospěch velkého rozsahu".*

Código penal[314], el *hacking* se encuentra regulado en su artículo 230, dedicado al acceso no autorizado a sistemas informáticos y soportes de información, dentro de su Título V, relativo a los delitos contra la propiedad. Su apartado primero castiga al que supere las medidas de seguridad para acceder a todo o parte de un sistema informático, incrementando las penas en su apartado segundo en el caso de que el sujeto que accede al sistema informático e injustificadamente utilice los datos almacenados, o bien los borre indebidamente, los dañe, cambie, suprima o reduzca su calidad, o los altere, o introduzca ilegalmente datos en el sistema informático.

El apartado 3 del precepto incrementa las penas para los casos en que exista intención de causar daño o pérdida o conseguir una ventaja injusta, o limitar indebidamente la funcionalidad del ordenador; el apartado 4 establece mayor castigo cuando se cometan las conductas de los apartados 1 o 2 como miembro de un grupo organizado, o bien causando daños considerables, se cause grave perturbación en empresa, autoridad, gobierno local, tribunal u otra autoridad pública, se obtenga para sí o para un tercero un beneficio sustancial, o se cause grave perturbación en un empresario. Por último, el apartado 5 incrementa las penas si los supuestos de los dos primeros apartados causan daños a gran escala o se obtiene para sí o para un tercero un beneficio a gran escala[315].

---

314 Disponible en www.mvcr.cz/soubor/sb011-09-pdf.aspx, consultado el 12 de enero de 2017.

315 *"§ 230 Neoprávněný přístup k počítačovému systému a nosiči*

*informací*

*(1) Kdo překoná bezpečnostní opatření, a tím neoprávněně získá přístup k počítačovému systému nebo k jeho části, bude potrestán odnětím svobody až na jeden rok, zákazem činnosti nebo propadnutím věci nebo jiné majetkové hodnoty.*

*(2) Kdo získá přístup k počítačovému systému nebo k nosiči informací a*

*a) neoprávněně užije data uložená v počítačovém systému nebo na nosiči informací,*

*b) data uložená v počítačovém systému nebo na nosiči informací neoprávněně vymaže nebo jinak zničí, poškodí, změní, potlačí, sníží jejich kvalitu nebo je učiní neupotřebitelnými,*

*c) padělá nebo pozmění data uložená v počítačovém systému nebo na nosiči informací tak, aby byla považována za pravá nebo podle nich bylo jednáno tak, jako by to byla data pravá, bez ohledu na to, zda jsou tato data přímo čitelná a srozumitelná, nebo*

*d) neoprávněně vloží data do počítačového systému nebo na nosič informací nebo učiní jiný zásah do programového nebo technického vybavení počítače nebo jiného technického zařízení pro zpracování dat, bude potrestán odnětím svobody až na dvě léta, záka zem činnosti nebo propadnutím věci nebo jiné majetkové hodnoty.*

*(3) Odnětím svobody na šest měsíců až tři léta, zákazem činnosti nebo propadnutím věci nebo jiné majetkové hodnoty bude pachatel potrestán, spáchá-li čin uvedený v odstavci 1 nebo 2*

*a) v úmyslu způsobit jinému škodu nebo jinou újmu nebo získat sobě nebo jinému neoprávněný prospěch, nebo*

*b) v úmyslu neoprávněně omezit funkčnost počítačového systému nebo jiného technického zařízení pro zpracování dat.*

*(4) Odnětím svobody na jeden rok až pět let nebo peněžitým trestem bude pachatel potrestán,*

*a) spáchá-li čin uvedený v odstavci 1 nebo 2 jako člen organizované skupiny,*

*b) způsobí-li takovým činem značnou škodu,*

*c) způsobí-li takovým činem vážnou poruchu v činnosti orgánu státní správy, územní samosprávy, soudu nebo jiného orgánu veřejné moci,*

*d) získá-li takovým činem pro sebe nebo pro jiného značný prospěch, nebo*

*e) způsobí-li takovým činem vážnou poruchu v činnosti právnické nebo fyzické osoby, která je podnikatelem.*

Por su parte, de forma similar a la establecida en el artículo 197 *ter* del Código español que se expondrá en el Capítulo IV, el artículo 231 castiga al sujeto que, con la intención de cometer los delitos del artículo 230, produce, pone en circulación, importa, exporta, transporta a través del país, ofrece, transmite, vende, pone a disposición para sí o para otro que lo adquiere o posee, un dispositivo, componente, proceso o herramienta, creado o adaptado para el acceso no autorizado a las redes de comunicaciones o a todo o parte de un sistema informático, o bien una contraseña, código de acceso, datos, procesos o cualquier otro medio similar por el que se puede obtener el acceso a todo o parte del sistema informático; incrementando las penas su apartado 2 en el caso de que el sujeto sea miembro de un grupo organizado para la comisión del delito, u obtenga un beneficio significativo para sí o para un tercero. Por último, su apartado 3 incrementa las penas si el infractor obtiene un beneficio sustancial para sí o para un tercero[316].

---

*(5) Odnětím svobody na tři léta až osm let bude pachatel potrestán,*
*a) způsobí-li činem uvedeným v odstavci 1 nebo 2 škodu velkého rozsahu, nebo*
*b) získá-li takovým činem pro sebe nebo pro jiného prospěch velkého rozsahu.".*

316 *"§ 231 Opatření a přechovávání přístupového zařízení a hesla k počítačovému systému a jiných takových dat*
*(1) Kdo v úmyslu spáchat trestný čin porušení tajemství dopravovaných zpráv podle § 182 odst. 1 písm. b), c) nebo trestný čin neoprávněného přístupu k počítačovému systému a nosiči informací podle § 230 odst. 1, 2 vyrobí, uvede do oběhu, doveze, vyveze, proveze, nabízí, zprostředkuje, prodá nebo jinak zpřístupní, sobě nebo jinému opatří nebo přechovává*
*a) zařízení nebo jeho součást, postup, nástroj nebo jakýkoli jiný prostředek,*

Por tanto, el Código checo anterior exigía la intención del sujeto de causar daños, perjuicio u obtener el beneficio injusto, intención que ya no exige el Código penal de 2009 para el tipo básico y, por otra parte, ni en uno ni en otro caso el Código establece las definiciones previas de los conceptos relativos al *hacking*, como se incluyen en el Convenio Europeo sobre Cibercriminalidad, la DM 2005/222/JAI y la Directiva 2013/40/UE. Sin embargo, destaca la mención en el nuevo Código del requisito relativo a la vulneración de medidas de seguridad en el acceso al sistema que exige el artículo 3 de la citada Directiva y que el anterior Código omitía. No obstante, el legislador sigue la línea expuesta de otras legislaciones europeas de incluir estos delitos entre los delitos contra la propiedad, con los consiguientes problemas interpretativos que puede originar en torno a cuál se considera como bien jurídico protegido por estos delitos, al que se dedica el siguiente Capítulo.

---

*včetně počítačového programu, vytvořený nebo přizpůsobený k neoprávněnému přístupu do sítě elektronických komunikací, k počítačovému systému nebo k jeho části, nebo*

*b) počítačové heslo, přístupový kód, data, postup nebo jakýkoli jiný podobný prostředek, pomocí něhož lze získat přístup k počítačovému systému nebo jeho části, bude potrestán odnětím svobody až na jeden rok, propadnutím věci nebo jiné majetkové hodnoty nebo zá- kazem činnosti.*

*(2) Odnětím svobody až na tři léta, zákazem činnosti nebo propadnutím věci nebo jiné majetkové hodnoty bude pachatel potrestán, a) spácháli čin uvedený v odstavci 1 jako člen organizované skupiny, nebo b) získáli takovým činem pro sebe nebo pro jiného značný prospěch.*

*(3) Odnětím svobody na šest měsíců až pět let bude pachatel potrestán, získáli činem uvedeným v odstavci 1 pro sebe nebo pro jiného prospěch velkého rozsahu*".

### *4.18 Rumanía.*

En este ámbito, el acceso a un sistema informático tenía su regulación específica en la Ley 161/2003[317], dirigida a garantizar la transparencia en la realización de altos cargos oficiales, posiciones públicas y empresariales, de prevención y sanción de la corrupción. En el Libro I, relativo a las provisiones generales para prevenir y luchar contra la corrupción, Título III que regulaba la prevención y lucha contra el cibercrimen, Capítulo I (previsiones generales), contenía entre sus definiciones la correspondiente al sistema informático y medidas de seguridad en su artículo 35[318], y en su Capítulo III (delitos y faltas), Sección 1 (delitos contra la confidencialidad e integridad de datos y sistemas informáticos), el artículo 42 castigaba en su tipo básico las conductas de acceso no autorizado a un sistema informático, sin exigir la vulneración de

[317] Ley 161/2003, de 19 de abril de 2003, disponible en http://legislatie.just.ro/Public/DetaliiDocument/71822, consultado el 12 de enero de 2017.

[318] La definición de sistema informático contenida en el artículo 35.a) era la de "*prin sistem informatic se înţelege orice dispozitiv sau ansamblu de dispozitive interconectate sau aflate în relaţie funcţională, dintre care unul sau mai multe asigura prelucrarea automată a datelor, cu ajutorul unui program informatic*", similar a la contenida el artículo 1 del Convenio Europeo sobre Cibercriminalidad, aprobado por el Consejo de Europa el 23 de noviembre de 2001 y se conceptuaban las medidas de seguridad en su apartado h) como "*prin măsuri de securitate se înţelege folosirea unor proceduri, dispozitive sau programe informatice specializate cu ajutorul cărora accesul la un sistem informatic este restrictionat sau interzis pentru anumite categorii de utilizatori*".

medidas de seguridad. El precepto incrementaba las penas en el caso de que existiera un propósito de obtener datos electrónicos y concluía estableciendo un mayor castigo en los supuestos de que unas u otras conductas se llevasen a cabo quebrantando medidas de seguridad.

Por su parte, el artículo 46 regulaba la producción, venta, importación, distribución o puesta a disposición, sin autorización, de contraseñas, código de acceso o cualquier otro dato electrónico que permita el acceso a todo o parte del sistema informático, o bien la posesión no autorizada de estos dispositivos o datos para cometer el delito. Por último, entre otros supuestos, el artículo 47 se ocupaba de la tentativa de acceso al sistema informático, llevando a la parte especial estos supuestos de delito intentado.

El Código penal aprobado por la Ley de 17 de julio de 2009[319] ha derogado los citados artículos 42, 46 y 47, estableciendo una definición de sistemas y datos informáticos idénticas a las del artículo 35.a) y 35.d) de la Ley 161/2003, en su artículo 181[320], si bien más

[319] Código Penal disponible en http://legislatie.just.ro/Public/DetaliiDocumentAfis/109854, consultado el 12 de enero de 2017.

[320] El artículo 181 del Código penal establece una definición de sistema y datos informáticos similar a la contenida en el artículo 1 del artículo 1 del Convenio Europeo sobre Cibercriminalidad. En concreto, establece el citado artículo: "*Sistem informatic şi date informatice.*
*(1) Prin sistem informatic se înţelege orice dispozitiv sau ansamblu de dispozitive interconectate sau aflate în relaţie funcţională, dintre care unul sau mai multe asigură prelucrarea automată a datelor, cu ajutorul unui program informatic.*
*(2) Prin date informatice se înţelege orice reprezentare a unor fapte, informaţii sau concepte într-o formă care poate fi prelucrată printr-un*

reducida para los datos informáticos[321].

El nuevo Código incluye los delitos de acceso a sistemas y datos informáticos en su artículo 360[322], ubicándolo entre los delitos contra la seguridad e integridad de los sistemas de información y datos (Capítulo VI), dentro del Título VII dedicados a los delitos contra la seguridad pública. El precepto tipifica el acceso no autorizado a un sistema informático, incrementándose las penas en su apartado dos para el supuesto de que el acceso fuera para obtener datos, y por último una pena mayor para los supuestos de acceso a través de procedimientos, dispositivos o programas restringidos o prohibidos para ciertas categorías de usuarios.

Por tanto, en el ámbito rumano no hay expresa referencia al mantenimiento en sistema informático ni a la necesaria vulneración de medidas de seguridad como sucede en el caso del Código español. Sin

---

*sistem informatic*".

321 La nueva definición de datos informáticos ya no incluye la referencia final a cualquier programa informático que pueda producir una función en el sistema informático "*În aceasta categorie se include şi orice program informatic care poate determina realizarea unei funcţii de către un sistem informatic*" que sí que incluye el artículo 35.d) de la Ley 161/2003.

322 El artículo 360 del Código penal rumano establece: *"Accesul ilegal la un sistem informatic*

*(1) Accesul, fără drept, la un sistem informatic se pedepseşte cu închisoare de la 3 luni la 3 ani sau cu amendă.*

*(2) Fapta prevăzută în alin. (1), săvârşită în scopul obţinerii de date informatice, se pedepseşte cu închisoarea de la 6 luni la 5 ani.*

*(3) Dacă fapta prevăzută în alin. (1) a fost săvârşită cu privire la un sistem informatic la care, prin intermediul unor proceduri, dispozitive sau programe specializate, accesul este restricţionat sau interzis pentru anumite categorii de utilizatori, pedeapsa este închisoarea de la 2 la 7 ani"*.

embargo, sigue el modelo de establecer definiciones con carácter previo a la tipificación de las conductas contenido en la normativa internacional, pero apartándose en su tipo básico de lo dispuesto en el artículo 3 de la Directiva 2013/40/UE, que incluye expresamente la "*violación de una medida de seguridad*".

Es destacable que el legislador rumano haya regulado los delitos de *hacking* en una sección propia con la Ley 161/2003, que llevaba por rúbrica los delitos contra la confidencialidad e integridad de datos y sistemas informáticos, y posteriormente en su Código Penal de 2009 en un capítulo dedicado a los delitos contra la seguridad e integridad de los sistemas de información y datos, en el título que se regulan los delitos contra la seguridad pública. Por ello, puede entenderse, conforme se expondrá en el Capítulo siguiente, que las rúbricas de la citada sección y capítulo son las que más se aproximan al bien jurídico protegido de estos delitos de entre las legislaciones europeas que se han expuesto.

### *4.19 Suecia.*

El Código penal sueco de 21 de diciembre de 1962[323] regula los accesos ilícitos en la sección 9.c de su capítulo 4 (delitos contra la

[323] Código penal disponible en https://www.riksdagen.se/sv/Dokument-Lagar/Lagar/Svenskforfattningssamling/Brottsbalk-1962700_sfs-1962-700/#K4, consultado el 12 de enero de 2017.

libertad y la paz), dentro de su parte segunda dedicada a los delitos en particular. En esta sección se castigaban las conductas de *hacking* tras la reforma introducida por Ley de 26 de abril de 2007, tipificando la conducta del que ilegalmente obtenía el acceso a una tarea diseñada para el procesamiento automatizado de datos o ilegalmente cambiara, eliminara, bloqueara o registrara esa tarea, castigando con iguales penas al que ilegalmente por cualquier otro medio similar perturbara o impidiera seriamente el uso de tal tarea[324].

Tras la Ley de 15 de mayo de 2014, el precepto sigue castigando en el tipo básico al sujeto que ilícitamente obtiene el acceso a una tarea con la que se pretende el tratamiento automatizado de datos o ilegalmente cambia, elimina, bloquea o registra esa tarea, de forma idéntica a la anterior regulación. Incluyendo iguales penas para el que ilegalmente por algún medio similar interrumpa o impida esa tarea, y concluyendo con mayores penas para los supuestos en los que el delito sea grave, atendiendo a si se ha causado grave daño, o ha afectado a un gran número de información[325].

---

[324] La sección 9 c modificada por la Ley de 26 de abril de 2007, establecía "*4 kap. 9 c §2 Den som i annat fall än som sägs i 8 och 9 §§ olovligen bereder sig tillgång till en uppgift som är avsedd för automatiserad behandling eller olovligen ändrar, utplånar, blockerar eller i register för in en sådan uppgift döms för dataintrång till böter eller fängelse i högst två år. Detsamma gäller den som olovligen genom någon annan liknande åtgärd allvarligt stör eller hindrar användningen av en sådan uppgift*", disponible en https://www.notisum.se/rnp/sls/sfs/20070213.pdf, consultado el 12 de enero de 2017.

[325] "*9 c § Den som olovligen bereder sig tillgång till en uppgift som är avsedd för automatiserad behandling eller olovligen ändrar, utplånar,*

Por tanto, el Código sueco no incluye las conductas de mantenimiento en el sistema previstas en el artículo 197 *bis* 1 del Código penal español, no se ocupa de establecer definiciones previas de los conceptos básicos que contiene el Convenio Europeo sobre Cibercriminalidad, la DM 2005/222/JAI y la Directiva 2013/40/UE, ni tampoco la vulneración de medidas de seguridad que exige el artículo 3 de esta Directiva, y sigue la línea de los países europeos que optan por no incluir los delitos informáticos en un capítulo o ley especial propia, regulando los supuestos de *hacking* entre los delitos contra la libertad y la paz.

## *5. CONCLUSIONES.*

Desde mi punto de vista, la mayoría de las legislaciones de los Estados miembros de la UE no son lo suficientemente minuciosas en materia de *hacking*, limitándose a regular el tipo básico, ni tampoco dotan a estas conductas de la debida autonomía respecto a otras, con

---

*blockerar eller i register för in en sådan uppgift döms för dataintrång till böter eller fängelse i högst två år. Detsamma gäller den som olovligen genom någon annan liknande åtgärd allvarligt stör eller hindrar användningen av en sådan uppgift. Är brottet grovt, döms för grovt dataintrång till fängelse i* lägst sex månader och högst sex år. *Vid bedömande av om brottet är grovt ska det särskilt beaktas om gärningen har orsakat allvarlig skada eller avsett ett stort antal uppgifter eller annars varit av särskilt farlig art*", disponible en https://www.notisum.se/rnp/sls/sfs/20140302.pdf, consultado el 12 de enero de 2017.

los consiguientes problemas interpretativos en cuanto al bien jurídico al que se dedica el siguiente Capítulo y que parecen tutelar los instrumentos europeos que inspiran la citada normativa.

Así, aunque como hemos visto algunos países realizan una loable extensa regulación del acceso a los sistemas informáticos y sus variantes (Croacia, Finlandia, Hungría, Malta, Portugal y Reino Unido), también es cierto que la mayoría de legislaciones europeas optan por tipificar el intrusismo informático junto a los delitos contra la intimidad (Alemania, Austria, Grecia y Polonia), entre los delitos contra el honor y otros derechos individuales (Dinamarca), contra la propiedad (Eslovaquia, Eslovenia, Estonia, Francia, Malta, República Checa y Luxemburgo), contra el orden público (Holanda), junto a otros delitos de daños (Irlanda), contra la inviolabilidad del domicilio (Italia), contra la libertad y la paz (Suecia), o contra la seguridad (Letonia, Lituania y Rumanía), y todos ellos plantean los problemas de delimitación del bien jurídico protegido con los citados delitos.

Frente a esos casos mayoritarios, se encuentran los países que han decidido regular sistemáticamente los delitos informáticos (Chipre, Portugal y Reino Unido) o, al menos, por dotarles de cierta autonomía en un título o capítulo propio y diferenciado (Bélgica, Bulgaria, Croacia, Finlandia o Hungría).

De todo ello resulta que son muy pocos los países que tipifican detalladamente el *hacking* y, además, lo hacen de forma sistemática y separada de otros delitos que no están relacionados con estas conductas. En concreto, los citados casos de Croacia, Finlandia,

Hungría, Portugal y Reino Unido. Además, entre ellos, es destacable que Hungría y Portugal ya regulasen esos supuestos incluso antes de ratificar en el año 2003 el Convenio Europeo sobre Cibercriminalidad.

Estos últimos casos demuestran que es posible una regulación ordenada de estos nuevos delitos, donde se incluyan unas definiciones de los conceptos esenciales, la regulación del tipo básico y sus modalidades y todo ello en una sola norma, título o capítulo propio, que no plantee la amalgama de artículos, remisiones y bienes jurídicos afectados que encuentra el intérprete del actual artículo 197 *bis* 1 CP, tal y como se viene anticipando y se expone en los siguientes capítulos.

# CAPÍTULO III.

# BIEN JURÍDICO PROTEGIDO Y OBJETO MATERIAL EN EL DELITO DE *HACKING.*

## *1. INTRODUCCIÓN.*

El artículo 197 *bis* 1 del CP establece:

*"El que por cualquier medio o procedimiento, vulnerando las medidas de seguridad establecidas para impedirlo, y sin estar debidamente autorizado, acceda o facilite a otro el acceso al conjunto o una parte de un sistema de información o se mantenga en él 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".*

Tal y como hemos visto, el texto del artículo 197 *bis* 1 trae causa del anterior 197.3 CP introducido en el Título X del Libro II del CP por la LO 5/2010. Es decir, está ubicado entre los *Delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio*. Por ello, los problemas de interpretación del anterior artículo 197.3 vuelven a repetirse con el nuevo artículo 197 *bis* 1, pues el legislador no ha atendido a las demandas de la mayoría de la doctrina de llevar a cabo una nítida separación.

En este Capítulo trataremos de clasificarlo. La primera cuestión es determinar si la aparición de los sistemas informáticos supone una nueva herramienta de alcance global que implica el nacimiento de nuevos bienes jurídicos que sean merecedores de protección penal o no.

Por lo general, podemos distinguir dos grupos de delitos relativos a los sistemas informáticos: el primero de ellos viene referido a los delitos cuya finalidad es la protección de esos sistemas

considerados como objeto material y el segundo grupo lo constituirían aquellos delitos relacionados con la utilización de los sistemas informáticos con fines delictivos.

Aunque algunos autores como FLORES PRADA[326] han defendido que lo relevante en cualquiera de estos delitos es conocer cómo la utilización de los sistemas informáticos puede llegar a vulnerar un bien jurídico protegido por el Derecho penal, declarando ORTS BERENGUER y ROIG TORRES que la informática constituye el medio habitual para la comisión de otros delitos[327], no cabe duda que ha existido una evolución en la tipificación de estas conductas, por cuanto en su descripción objetiva incorporan la idea del ataque a un bien jurídico que hasta ahora necesitaba de otras referencias típicas para ser identificado[328]. Como novedad desde la LO 1/2015 también se tipifican delitos consistentes en facilitar esas conductas, que como indican MUÑOZ CUESTA y RUIZ DE ERENCHUN completan la tutela del bien jurídico protegido por esos delitos[329] y como señala COLÁS TURÉGANO suponen un adelanto de las barreras de protección del bien jurídico protegido[330], aspecto positivo de la

---

326 FLORES PRADAS, I., *Criminalidad informática (Aspectos sustantivos y procesales)*, ed. Tirant Lo Blanch, primera edición, Valencia, 2012, p. 41.

327 ORTS BERENGUER, E. y ROIG TORRES, M., *Delitos informáticos y delitos comunes ...*, *cit*., nota 112, p. 13.

328 En este sentido, MORALES GARCÍA, O., "Delincuencia informática: instrusismo, ...", cit. nota 142, p. 185.

329 MUÑOZ CUESTA, J. y RUIZ DE ERENCHUN ARTECHE, E., *Cuestiones prácticas sobre la reforma penal de 2015*, ed. Aranzadi, primera edición, Navarra, 2015, p. 145.

330 COLÁS TURÉGANO, A., "Nuevas conductas delictivas ...", *cit*., nota

reforma en cuanto se otorga una mayor cobertura a las distintas variantes del fenómeno *hacking* y a la vez suponen un paso más en su configuración como un delito independiente de los delitos contra la intimidad, pero que tiene como contrapartida el hecho de que el legislador no se haya preocupado de evitar más claramente su posible colisión con las conductas de facilitar el acceso previstas en el artículo 197 *ter* CP a las que se dedica el Capítulo siguiente.

Tal y como veremos a continuación, de acuerdo con la clasificación mencionada, el sistema informático en sí mismo considerado como bien jurídico protegido puede tener tanta trascendencia como su utilización para lesionar otro bien jurídico protegido. Esa heterogeneidad de bienes jurídicos protegidos es lo que probablemente fundamenta la dispersión de estas conductas en el Código Penal[331].

Con estas premisas, en el presente Capítulo se trata de realizar una aproximación al bien jurídico protegido y al objeto material en el delito de intrusismo informático.

---

168, p. 664.

331 ORTS BERENGUER, E. y ROIG TORRES, M., *Delitos informáticos y delitos comunes ...*, *cit*., nota 112, p. 14.

## *2. PLANTEAMIENTO.*

Siguiendo a CARBONELL MATEU[332], el principio general de libertad en el Derecho penal se encuentra proclamado en los artículos 1 y 10 de la Constitución española[333], a lo que se añade que el citado principio implica que sólo puede prohibirse lo que restringe el libre desarrollo de la personalidad de los ciudadanos, es decir, las libertades sólo se podrán limitar para proteger las libertades de las demás personas y sólo en la medida de lo necesario. Como manifestaciones de ese principio se encuentran otros: el principio de adecuación, que exige que el Derecho penal sea un medio adecuado para salvaguardar el bien jurídico y que la medida elegida sea apta para el fin perseguido; el principio de necesidad, que prohíbe el exceso, considerándose injusta la pena que es innecesaria; el principio de proporcionalidad, por el cual se debe ponderar la gravedad de la conducta, el objeto de protección y la consecuencia jurídica, debiendo tener el bien jurídico la suficiente importancia como para justificar la

---

332 CARBONELL MATEU, J. C., "Reflexiones sobre el abuso del Derecho penal y la banalización de la legalidad", en ARROYO ZAPATERO, L. A. y BERDUGO GÓMEZ DE LA TORRE, I. (Coords.), *Homenaje al Dr. Marino Barbero Santos: "in memoriam"*, ed. Universidad de Castilla-La Mancha, Cuenca, 2001, pp. 131-134.

333 Como sabemos, los artículos 1.1 y 10.1 CE establecen, respectivamente, "*España se constituye en un Estado social y democrático de Derecho, que propugna como valores superiores de su ordenamiento jurídico la libertad, la justicia, la igualdad y el pluralismo político*" y "*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*".

privación de libertad; y el principio de ofensividad u ofensión, por el cual no puede haber delito si no existe la vulneración o peligro para un bien jurídico. Este último principio supone que desde una concepción imperativa de la norma el *ius puniendi* del Estado queda limitado porque no se deberán prohibir determinados comportamientos si no es porque son lesivos para el bien jurídico, mientras que desde una consideración valoradora de la norma el principio de ofensión de toda norma penal resultará que existe un bien jurídico, y habrá que atender a la dignidad del bien jurídico para que el citado principio de ofensividad pueda recuperar su razón de ser como limitador de ese poder punitivo. Es decir, no tanto atender a la inaplicación de la pena si no hay lesión del bien jurídico, sino que el legislador no tipifique conductas que no sean precisas para la protección de un bien jurídico digno de tutela penal, y será la Constitución la norma valoradora por excelencia que determine los valores a proteger. Y, además de esa dignidad formal, se hace precisa la material en el principio de ofensión, es decir, que el valor esté aceptado socialmente, siendo posible su lesión o puesta en grave peligro y necesitado de protección penal.

Por tanto, tal y como indicaba WELZEL, para que una acción pueda considerarse delito es necesario que infrinja un determinado orden de la comunidad o elemento valioso de la vida social[334].

Los bienes jurídicos protegidos han sido considerados como el

[334] WELZEL, H., *El nuevo sistema del Derecho penal*, ed. B de F, cuarta reimpresión, Buenos Aires, 2011, traducido por CEREZO MIR, J., pp. 69 y 75.

interés jurídicamente protegido, siendo todos ellos intereses vitales del individuo o de la comunidad[335]; o también el interés o valor que motiva la tipificación como delito de tal conducta[336].

Una corriente doctrinal, denominada conservadora y positivista[337] lo ha descrito como todo objeto que la ley penal en los respectivos tipos considera digno de protección, de esta forma, el catálogo de bienes jurídicos resulta de la ley y se define en la ley. En este sentido se puede conceptuar como cualidad positiva que el legislador atribuye a determinados intereses, que la ley quiere proteger de las conductas que pueden dañarlo, siendo en consecuencia creado por la ley y no algo prexistente a ella[338].

Frente a esta corriente, se encuentra la que entiende que el bien jurídico es prexistente e independiente a su reconocimiento por la ley.

Sin ánimo de analizar ahora los argumentos a favor de una u otra dirección, que no constituyen el objeto de la presente obra, esta última postura es la mayoritaria en la doctrina, corriente que LUZÓN PEÑA[339] denomina crítica y reformista y que lo definiría como el

---

335 VON LISZT, F., *Tratado de Derecho penal*, Tomo II, ed. Reus, segunda edición, Madrid, 1927, traducido por JIMÉNEZ DE ASÚA, L., p. 2.

336 RODRÍGUEZ RAMOS, L., *Compendio de Derecho Penal. Parte General*, ed. Dykinson, 2ª edición, Madrid, 2010, p. 113.

337 En este sentido se refiere a esta doctrina LUZÓN PEÑA, D. M., *Lecciones de Derecho penal. Parte General*, ed. Tirant lo Blanch, tercera edición, Valencia, 2016, p. 168.

338 MUÑOZ CONDE, F., y GARCÍA ARÁN, M., *Derecho Penal. Parte General*, ed. Tirant lo Blanch, 9ª edición, Valencia, 2015, p. 276.

339 LUZÓN PEÑA, D. M., *Lecciones de Derecho penal ...*, *cit*., nota 337, pp. 168 y 169.

interés, valor o realidad valiosa, de una persona o de la sociedad, importante para su existencia y desenvolvimiento y que por ello merece protección jurídica. Para este autor sin embargo parece más acertado describir el bien jurídico en un sentido amplio, como condiciones necesarias para el desarrollo de la vida del individuo y de la sociedad.

Por tanto, es el objeto de protección contra el que se dirige la conducta delictiva, por lo que sólo es imaginable su tutela mediante la incorporación de un modo de menoscabo[340].

Por ello, no debe confundirse ese bien jurídico, considerado interés medio que toma en cuenta el Derecho, objeto de protección de la ley u objeto de ataque contra el que se dirige el delito, con el objeto de protección u objeto corporal sobre el que la acción se realiza, objeto material al que se dedica el epígrafe 4 de este Capítulo. Así, como indicaba MEZGER, el bien jurídico lo constituye el valor objetivo al que la ley penal concede su protección[341].

De esta forma, como señala BOIX REIG[342], el hecho de

---

340 WELZEL, H., *Estudios de Derecho penal*, ed. B de F, reimpresión, Buenos Aires, 2007, traducido por EDUARDO ABOSO, G., y LOW, T., p.46-47, 50.

341 MEZGER, E., *Tratado de Derecho penal*, Tomo I, ed. Revista de Derecho privado, segunda edición, Madrid, 1933, traducido por RODRÍGUEZ MUÑOZ, J.A., p. 333.

342 BOIX REIG, J., "Consideraciones sobre la protección penal de la intimidad y del honor e informática", en *Anales de la Universidad de Alicante. Facultad de Derecho*, 1983, 2, p. 32. Disponible en https://rua.ua.es/dspace/bitstream/10045/55007/1/Anales_Fac_Derecho_02_02.pdf, consultado el 27 de septiembre de 2016.

comprobar la existencia de un objeto merecedor de protección y que han aparecido mecanismos tecnológicos que los ponen en posición debilitada evidencia la necesidad de nuevas normas penales.

La citada definición de bien jurídico expuesta por MEZGER es la que se va a seguir en el presente trabajo y nos va a permitir conocer los límites del *ius puniendi* del Estado, por cuanto es la que permite exigir tipos penales cuando se vean afectados bienes jurídicos individuales o colectivos y no sólo cuando una conducta sea considerada meramente inmoral. De esta forma, será posible una interpretación restrictiva del tipo penal y excluir una interpretación amplia que admitiría el tenor literal del artículo 197 *bis* 1 CP dando lugar a incluir conductas que no afectan al bien jurídico protegido y que deben ser excluidas del ámbito de la tipicidad.

En consecuencia, en el presente trabajo se analiza cuál es el bien jurídico protegido en el nuevo delito de *hacking* y si con la reforma de la LO 1/2015 el legislador ha cumplido con el principio de intervención mínima y las directrices que le venían impuestas por la UE a través de la Directiva 2013/40/UE, por cuanto como señala MIR PUIG[343], todo Código penal supone la realización de un programa político-criminal que tiene entre sus fundamentos la determinación de los bienes dignos de protección.

Esa determinación del bien jurídico protegido la obtendremos mediante la interpretación. De esta forma, una vez conocido ese bien

[343] MIR PUIG, S., *Derecho penal. Parte general*, ed. Reppertor, décima edición, Barcelona, 2016, p. 173.

tendremos, a la vez, lo que autores como MEZGER han considerado el principal medio de interpretación del tipo y sus características[344].

Por otra parte, el bien jurídico protegido también permitirá conocer si es adecuada la ubicación del artículo 197 *bis* 1 en el Libro II, Título X, Capítulo I, en lo que se denomina la función sistemática[345], la exclusión de las conductas que no pongan en peligro o lesionen ese bien jurídico y facilitará en la práctica la medición de la pena en función de su mayor o menor lesión teniendo en cuenta el margen que se concede a los órganos jurisdiccionales por el artículo 66.1.6º del CP[346].

Desde estas premisas se intenta analizar en el presente trabajo si el bien jurídico tutelado en el artículo 197 *bis* 1 del CP cumple la función que tiene y se han respetado los límites establecidos por la Directiva 2013/40/UE que le trae causa.

---

344 MEZGER, E., *Tratado de Derecho penal* ..., *cit*., nota 341, p. 334.

345 MIR PUIG, S., *Derecho penal* ..., *cit*., nota 343, p. 175. También en este sentido, LUZÓN PEÑA, D. M., *Lecciones de Derecho penal* ..., *cit*., nota 337, p. 170.

346 Artículo 66.1.6º CP: "*En la aplicación de la pena, tratándose de delitos dolosos, los jueces o tribunales observarán, según haya o no circunstancias atenuantes o agravantes, las siguientes reglas: 6º Cuando no concurran atenuantes ni agravantes aplicarán la pena establecida por la ley para el delito cometido, en la extensión que estimen adecuada, en atención a las circunstancias personales del delincuente y a la mayor o menor gravedad del hecho.".*

## *3. EL DELITO DE HACKING COMO DELITO CONTRA LA INTIMIDAD.*

### *3.1 Introducción.*

El planteamiento del bien jurídico protegido en el caso de estas conductas condiciona el enfoque de problemas tales como la exigencia o no de una finalidad jurídica añadida a la simple curiosidad o demostración de pericia informática que pueda tener un *hacker* y si resulta necesario o no adelantar la barrera de intervención del Derecho penal para tipificar estas conductas como un delito autónomo[347].

Atendida la denominada función sistemática que cumple el bien jurídico protegido, en el presente apartado vamos a intentar dilucidar si el delito de *hacking* forma parte de los delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio, considerando la ubicación sistemática del artículo 197 *bis* 1 del CP.

El precepto se sitúa sistemáticamente entre los citados delitos, es decir, en el Título X del Libro II del CP. Más concretamente en su Capítulo I, dedicado al "*descubrimiento y revelación de secretos*". Por

[347] En este sentido, RUEDA MARTÍN, M. Á., "Los ataques contra los sistemas informáticos: conductas de hacking. Cuestiones político-criminales", en ARMAZA ARMAZA, Emilio José (Coord.), y VVAA, *La Adaptación del Derecho Penal al Desarrollo Social y Tecnológico*, ed. Comares, Granada, 2010, p. 362.

tanto, el lugar donde se encuentra el citado precepto es el mismo que el de su predecesor, el artículo 197.3 introducido con la LO 5/2010.

Todo ello sin perjuicio de que con la reforma de 2010 el *hacking* estaba tipificado incluso dentro del mismo precepto de otros delitos contra la intimidad y tras la LO 1/2015 la regulación del instrusismo informático se realiza en un precepto autónomo. Así, según expone el legislador en el Preámbulo de esta última reforma:

"*se introduce una separación nítida entre los supuestos de revelación de datos que afectan directamente a la intimidad personal, y el acceso a otros datos o informaciones que pueden afectar a la privacidad pero que no están referidos directamente a la intimidad personal: no es lo mismo el acceso al listado personal de contactos, que recabar datos relativos a la versión de software empleado o a la situación de los puertos de entrada a un sistema. Por ello, se opta por una tipificación separada y diferenciada del mero acceso a los sistemas informáticos*"[348].

Sin embargo, aunque el legislador se refiera a una "*separación nítida*" entre los delitos que afectan directamente a la intimidad personal y el acceso a datos o informaciones que no están referidos directamente a la intimidad personal, lo cierto es que estas conductas siguen estando en el mismo Capítulo que los citados delitos.

[348] Preámbulo de la LO 1/2015, BOE nº 77, de 31 de marzo de 2015, apartado XIII.

Por ello, hemos de atender a si la intimidad[349] constituye o no el objeto de protección en este delito, razón por la cual se hace necesario considerar el objeto de tutela común en los delitos contra la intimidad[350] a los efectos de analizar si el vigente artículo 197 *bis*.1 del CP cumple o no con las mismas estructuras. Para ello, me voy a ocupar de realizar un acercamiento al bien jurídico común de los delitos contra la intimidad y su evolución histórica, para concluir con lo que considero el bien jurídico protegido por el delito que estamos tratando, su objeto material y su naturaleza.

### *3.2 Aproximación al bien jurídico común de los delitos contra la intimidad.*

Como se ha expuesto en anteriores apartados, el derecho a la intimidad es un derecho fundamental que se encuentra reconocido en el artículo 18 de la Constitución española. Por tanto, le acompañan todas las garantías constitucionales de tutela de estos derechos,

---

349 Como indica QUERALT JIMÉNEZ, J. J., *Derecho Penal Español ..., cit.*, nota 162, p. 283-284, la ubicación sistemática del precepto lleva a plantearnos ese objeto de protección.

350 Desde el primer momento el Consejo de Ministros en su referencia de 14 de julio de 2006 al Anteproyecto parece inclinarse porque el bien jurídico protegido en el acceso ilícito es la intimidad, separando los delitos contra la intimidad de los delitos de daños en los siguientes términos: "*Se caracterizan como delitos las intromisiones ilegales en sistemas informáticos ajenos (hackers). Se castigarán tanto los ataques contra la intimidad, como los posibles delitos por daños que puedan producir grave perjuicio a empresas u organismos públicos*".

especialmente las relativas a la reserva de ley orgánica, su tutela ante los tribunales ordinarios por un procedimiento preferente y sumario y ante el Tribunal Constitucional a través del recurso de amparo, quien, como veremos a continuación, ha reconocido como facultades derivadas de este derecho tanto el derecho de excluir a terceros del círculo propio como el derecho de control sobre los datos personales.

En el ámbito penal, el Título X del Libro II del CP está dedicado a las conductas que pueden atentar contra la intimidad y, dentro de este Título, el Capítulo I agrupa los artículos 197 a 201 bajo la rúbrica "*Del descubrimiento y revelación de secretos*".

La ubicación del delito de *hacking* entre los delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio ha generado numerosas críticas, algunas de las cuales se expondrán en los siguientes apartados, fundamentalmente por entender que con la tipificación del *hacking* a través de la LO 5/2010 primero y con la LO 1/2015 después, no se tutela necesariamente la intimidad.

Esta organización sistemática por nuestro legislador supone un tratamiento unitario del derecho a la intimidad en el Código penal, que siguiendo el esquema de NUÑEZ CASTAÑO[351] tendría la siguiente estructura: (i) el acceso ilícito o no permitido a la intimidad, donde se

[351] NUÑEZ CASTAÑO, E. "Lección XII. Delitos contra la intimidad el derecho a la propia imagen y la inviolabilidad del domicilio", en GÓMEZ RIVERO, M. C. (Coord.) y VVAA., *Nociones Fundamentales de Derecho Penal*, ed. Tecnos. Madrid, 2010, p. 225.

incluirían sus artículos 197 y 198 y, tras la reforma de la LO 1/2015, habría que incorporar los artículos 197 *bis*, 197 *ter*, 197 *quater* y 197 *quinquies*; (ii) la revelación de secretos por el obligado a guardarlos, que comprende su artículo 199; (iii) el acceso no autorizado a datos de personas jurídicas previsto en su artículo 200; y (iv) la condición para la perseguibilidad de estos delitos en el artículo 201.

De esta forma, con la regulación de estas conductas en el Título X, se trata de proteger en el ámbito penal la intimidad frente a las intromisiones de los demás en la vida privada de un sujeto[352], además del secreto, el *habeas data* y el derecho a la propia imagen. La intimidad individual es el bien jurídico protegido en el artículo 197 del CP, circunstancia que se pone de manifiesto por su ubicación en este Título[353], de tal forma que como indican ORTS BERENGUER y ROIG TORRES, las acciones que se describen han de recaer sobre datos, documentos, efectos, imágenes o sonidos, relevantes para la intimidad[354]. Este es también el bien jurídico que podemos considerar protegido de forma unitaria en el citado Título siguiendo el criterio jurisprudencial. Así, en cuanto al bien jurídico en el artículo 197.1 CP, la jurisprudencia considera como tal la intimidad personal garantizada

352 QUERALT JIMÉNEZ, J. J., *Derecho penal español ...*, *cit*., nota 162, p. 283.

353 En este sentido, RODRÍGUEZ RAMOS, L. (Dir.) y VVAA, *Código Penal. Concordado y comentado con jurisprudencia y leyes penales especiales y complementarias*, ed. La Ley, quinta edición, Madrid, 2015, p. 1081.

354 ORTS BERENGUER, E. y ROIG TORRES, M., *Delitos informáticos y delitos comunes ...*, *cit*., nota 112, p. 20.

en el artículo 18.1 de la Constitución[355], entendida como la vertiente clásica o negativa de la intimidad en cuanto derecho de exclusión[356], y en el caso del artículo 197.2 CP también se ha coincidido en señalar que se trata de "*delitos contra la intimidad de las personas mediante el uso de la informática y de las comunicaciones*"[357], si bien en este último caso, de forma más acorde con la evolución del derecho a la intimidad, podemos entender que las conductas del apartado 2 implican abusos informáticos contra la *privacy* o libertad informática[358], entendida como derecho de control sobre los datos personales propios, vertiente positiva o *habeas data* que para autores como TOMÁS-VALIENTE LANUZA podría considerarse un nuevo derecho fundamental[359].

### *3.2.1 Evolución histórica.*

En síntesis, en nuestro ordenamiento jurídico interno el artículo 18.1 CE dispone:

---

355 Entre otras, STS 694/2003 de 20 de junio de 2003, recurso 2667/2001, Pte. Ilmo. Sr. D. Eduardo Móner Muñoz (RJ 2003\4359), FJ 5º.

356 TOMÁS-VALIENTE LANUZA, C., "Título X. Delitos contra la Intimidad ...", *cit*., nota 127, p. 794.

357 CARBONELL MATEU, J. C. y GONZÁLEZ CUSSAC, J. L., "Delitos contra la Intimidad, el Derecho a la Propia Imagen y la Inviolabilidad del Domicilio", en VVAA, *Derecho Penal. Parte especial,* ed. Tirant Lo Blanch, Valencia, 2010, *CD-ROM*.

358 MORÓN LERMA, E., *Internet y Derecho penal ..., cit*., nota 5, p. 61.

359 TOMÁS-VALIENTE LANUZA, C., "Título X. Delitos contra la Intimidad ...", *cit*., nota 127, p. 794.

"*Se garantiza el derecho al honor, a la intimidad personal y familiar y a la propia imagen*" y en el artículo 18.4 CE se dice:

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

Con estas premisas, el derecho a la intimidad no se concibe sólo como un derecho a la exclusión de terceros sobre la información personal según la concepción tradicional[360], sino que como declaraba la STC 254/1993, de 20 de julio, también incluye el aspecto positivo de poder controlar los datos personales que circulan a través de los sistemas informáticos. Así, esta Sentencia analizaba el derecho a la intimidad tanto desde el punto de vista tradicional, negativo, considerándolo un derecho de exclusión de los terceros sobre los datos personales, como desde un punto de vista positivo, comprendiendo el conocimiento de la existencia de ficheros con datos personales, sus fines y los responsables de los mismos, lo que conlleva un derecho de información de los ciudadanos ante las Administraciones públicas como parte de su derecho fundamental a la intimidad[361].

---

360 STC 143/1994, Sala Primera, de 9 de mayo de 1994, Recurso de Amparo núm. 3192/1992, Pte. Ilmo. Sr. D. Miguel Rodríguez-Piñero y Bravo-Ferrer (RTC 1994\143), FJ 6º: la privacidad "*implica la existencia de un ámbito propio y reservado frente a la acción y el conocimiento de los demás, necesario, según las pautas de nuestra cultura, para mantener una calidad mínima de la vida humana*".

361 STC 254/1993, Sala Primera, de 20 de julio de 1993, Recurso de Amparo núm. 1827/1990, Pte Ilmo. Sr. D. Fernando García-Mon y González Regueral (RTC 1993\254), FJ 7: "*Esta constatación elemental de que los*

Todo ello supone, por tanto, un cambio sobre el derecho a la intimidad que inicialmente comprendía el derecho *to be let alone* o de exclusión y que explicaban en sus orígenes, en el año 1890, WARREN y BRANDEIS[362] como el siguiente paso en la evolución de la protección del hombre, exigido por los cambios políticos, sociales y económicos, que implican el reconocimiento de nuevos derechos, con la tutela de la naturaleza espiritual del hombre, sus sentimientos y su intelecto, ampliándose el alcance de sus derechos, llegando a significar el derecho a la vida la facultad de disfrutarla, el derecho a estar solo, a dejarse llevar. Las recientes invenciones y métodos comerciales llaman la atención sobre el siguiente paso para la protección de la personas, debiéndose asegurar el derecho a estar solo, especialmente por las recientes invasiones en los ámbitos privados de

---

*datos personales que almacena la Administración son utilizados por sus autoridades y sus servicios impide aceptar la tesis de que el derecho fundamental a la intimidad agota su contenido en facultades puramente negativas, de exclusión. Las facultades precisas para conocer la existencia, los fines y los responsables de los fiches* (sic) *automatizados dependientes de una Administración pública donde obran datos personales de un ciudadano son absolutamente necesarias para que los intereses protegidos por el art. 18 CE, y que dan vida al derecho fundamental a la intimidad, resulten real y efectivamente protegidos. Por ende, dichas facultades de información forman parte del contenido del derecho a la intimidad, que vincula directamente a todos los poderes públicos, y ha de ser salvaguardado por este Tribunal, haya sido o no desarrollado legislativamente [STC 11/1981, fundamento jurídico 8º, y 101/1991 (RTC 1991\101), fundamento jurídico 2ª]*".

362 WARREN, S. D. y BRANDEIS, L. D., "The right to privacy", en Harvard Law Review, Vol. IV, de 15 de diciembre de 1890, nº 5, disponible en http://groups.csail.mit.edu/mac/classes/6.805/articles/privacy/Privacy_brand_warr2.html, consultado el 15 de enero de 2017.

la vida doméstica provocadas por las fotografías instantáneas y los periódicos.

Ese derecho inicial da paso poco a poco con la evolución de las nuevas tecnologías a un nuevo *habeas data* que abarca el control sobre los datos informatizados. Como indica MORALES PRATS, tras la Segunda Guerra Mundial, las amenazas gubernativas sobre las esferas de intimidad de las personas no paran de incrementarse. Así, la lealtad al sistema implica un permanente control sobre el ciudadano a través de la información, manejándose tanto en el ámbito público como privado sus datos personales como forma de dominio. Esos datos se convierten en bienes de mercado. Surge como novedad el poder informático, como método de información, pero que puede suponer un control virtual. De esta forma en la década de los años sesenta se toma conciencia del desfase en torno a la consideración clásica del derecho a la intimidad, pues hasta entonces se consideraba que sólo eran posibles las injerencias físicas. Frente al derecho a la propia imagen y al secreto de las comunicaciones reconocidos recientemente como consecuencia de las máquinas de grabación, surge la conciencia del peligro de la recogida y tratamiento informático de datos, por cuanto los ordenadores hacen posible multiplicar el poder de la información, siendo los datos personales el citado valor de mercado. Con la evolución de las nuevas tecnologías en los años setenta crecen las nuevas amenazas para la libertad de las personas en dos ámbitos: la participación democrática en el control y acceso a las informaciones y la protección de la esfera íntima. La

información no queda ya en la memoria del que la recaba o en los medios físicos tradicionales, sino en un sistema informático. Por ello, se hace precisa la elaboración del régimen de la intimidad, que exigía la protección de la esfera íntima del individuo como garantía para poder llevar a cabo otras libertades, el derecho a la *privacy* se manifiesta como el derecho al control sobre la circulación de informaciones personales, las facultades de exclusión se proyectan actualmente también sobre los bancos de datos, el *habeas mentem* que surge con las primeras técnicas de control audiovisual se traduce en *habeas data*, empezando a tipificarse el acceso a esos bancos de datos, incluyéndose el derecho al control sobre la recogida de las informaciones personales. Es decir, se reconoce el derecho del sujeto a modificar su identidad informática para hacerla veraz. Por último, este nuevo grupo de derechos va acompañado de las necesarias reformas legislativas que garanticen su protección[363].

De esta forma, el derecho reconocido en el artículo 18.4 CE se concibe actualmente como un derecho que comprende "*los derechos a la intimidad y al honor y del pleno disfrute de los derechos de los ciudadanos que, además, es en sí mismo un derecho o libertad fundamental, el derecho a la libertad frente a las potenciales agresiones a la dignidad y a la libertad de la persona provenientes de un uso legítimo del tratamiento mecanizado de datos, lo que la*

[363] MORALES PRATS, F., *La tutela penal de la intimidad: privacy e informática*, ed. Destino, Barcelona, 1984, p. 15-45.

*Constitución llama la informática*"[364]. Por ello, ahora se hace referencia a este derecho como libertad informática, de tal manera que "*la garantía de la vida privada de la persona y de su reputación poseen hoy una dimensión positiva que excede el ámbito propio del derecho fundamental de la intimidad (art. 18.1 CE), y que se traduce en un derecho de control sobre los datos relativos a la persona. La llamada "libertad informática" es así un derecho a controlar el uso de los datos insertos en un programa informático (habeas data) y comprende, entre otros aspectos, la oposición del ciudadano a que determinados datos personales sean utilizados para fines distintos de aquél legítimo que justificó su obtención*"[365].

Esta interpretación del derecho reconocido en el artículo 18.4 CE tiene en común con el derecho reconocido por el artículo 18.1 CE el objetivo de ofrecer una efectiva tutela constitucional de la vida privada personal y familiar[366]. Sin embargo, el apartado 4 a su vez atribuye al titular del derecho un poder para imponer a terceros determinados comportamientos u omisiones que se regulan y desarrollan legalmente para limitar el uso de la informática. Como indica ANARTE BORRALLO, aunque los datos hayan escapado del

---

364 STC 292/2000, Pleno 30 de noviembre de 2000, Recurso de Amparo núm. 1463/2000, Pte. Ilmo. Sr. D. Julio Diego González Campos (RTC 2000\292), FJ 5º.

365 *Ibíd.,* FJ 5º.

366 Según pone de relieve FRÍGOLS I BRINES, E., en "La protección constitucional de los datos de las comunicaciones", en BOIX REIG, J. (Dir.) y JAREÑO LEAL, A. (Coord.), *La protección jurídica de la intimidad*, ed. Iustel, Madrid, 2010, p. 41, el artículo 18 CE "*contiene lo que se configura como una protección integral de la esfera privada del ciudadano*".

ámbito del dominio material o informático de su titular, sigue teniendo un poder jurídico de control sobre ellos, que le faculta genéricamente para dirigir su circulación, su integridad y su manipulación[367]. Así, mientras el derecho a la intimidad del artículo 18.1 CE protege al individuo frente a cualquier invasión al ámbito de su vida personal y familiar por parte de terceros, según la misma STC 292/2000, FJ 6º, "*el derecho fundamental a la protección de datos persigue garantizar a esa persona un poder de control sobre sus datos personales, sobre su uso y destino, con el propósito de impedir su tráfico ilícito y lesivo para la dignidad y derecho del afectado*" o, de forma más tajante, mientras "*el derecho a la intimidad permite excluir ciertos datos de una persona del conocimiento ajeno (...) es decir, el poder de resguardar su vida privada de una publicidad no querida*", sin embargo, "*el derecho a la protección de datos garantiza a los individuos un poder de disposición sobre esos dat*os".

Por lo que respecta a la tutela penal de estos derechos, la inclusión de estos delitos constituye una de las novedades del Código Penal de 1995, superando su consideración como ilícito administrativo. Con anterioridad a 1995 la regulación de esta materia se llevaba a cabo en la Ley Orgánica 5/1992, de 29 de octubre, relativa al Tratamiento Automatizado de Datos de Carácter Personal, que fue sustituida en el ámbito administrativo por la Ley Orgánica

[367] ANARTE BORRALLO, E., "Sobre los límites de la protección penal de datos personales", en *Derecho y conocimiento: anuario jurídico sobre la sociedad de la información y del conocimiento*, nº 2, ed. Facultad de Derecho de la Universidad de Huelva, Huelva, 2002, p. 230.

15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal y que incorporaba como novedad la ampliación del campo de protección de los datos de carácter personal con independencia del soporte en el que se incorporaran.

Toda esta protección responde a la necesidad de que el Estado Social y Democrático de Derecho garantice los derechos reconocidos en el artículo 18 CE, lo que exige establecer un ámbito en el que el individuo pueda desarrollar su privacidad sin injerencias ajenas, dentro del espacio que la persona elige[368].

Uno de los méritos del CP de 1995, tal y como señala MORALES PRATS[369] fue precisamente la organización en un solo Título de las diversas figuras delictivas que estaban dispersas en el anterior Código, dotando de unidad y coherencia sistemática a los delitos contra la intimidad, si bien la rúbrica más correcta para este autor habría sido la referencia exclusivamente a "delitos contra la intimidad", considerando que la propia imagen o el allanamiento de morada, como intimidad domiciliaria, serían alusiones innecesarias si lo tutelado es la intimidad en sentido amplio.

Por tanto, los delitos del artículo 197 CP tienen en común la

---

368 COTS MARFIL, A., "Una aproximación al artículo 197.2 del Código Penal vigente", en *AJA,* nº 757/2008, Pamplona, 2008, p. 9.

369 MORALES PRATS, F., "Título X. Delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio", en QUINTERO OLIVARES, G. (Dir.), MORALES PRATS, G. (Coord.), *Comentarios a la Parte especial del Derecho penal*, ed. Aranzadi, novena ed., Navarra, 2011, p. 448 y 449.

protección de la intimidad, valor que tiene mayor amplitud que el secreto y que no debe confundirse con éste, tal y como veremos en el siguiente subepígrafe.

Con este punto de partida, debemos recordar que con la reforma llevada a cabo por la LO 5/2010 se ha introducido una nueva conducta en el artículo 197.3, según su Preámbulo, "*para cumplimentar la Decisión Marco 2005/222/JAI, de 24 de febrero de 2005, relativa a los ataques contra los sistemas de información, se ha resuelto incardinar las conductas punibles en dos apartados diferentes, al tratarse de bienes jurídicos diversos*"[370], trasladada al artículo 197 *bis* 1 tras la LO 1/2015, consistente en el acceso no autorizado a un sistema informático y que tiene más difícil encaje con la intimidad, por cuanto se tipifica el mero acceso o mantenimiento en un sistema informático, sin autorización y vulnerando las medidas de seguridad establecidas.

Entre la doctrina se ha discutido cuáles son los bienes jurídicos objeto de tutela a los que se refería el citado Preámbulo de la LO 5/2010, señalando HERNÁNDEZ DÍAZ al menos los siguientes[371]:

(i) Seguridad informática.

La seguridad informática se entendería como un bien jurídico colectivo, no disponible individualmente, con el que finalmente se trataría de proteger otros de naturaleza individual (honor e intimidad

370 Apartado XIV del Preámbulo de la LO 5/2010.

371 HERNÁNDEZ DÍAZ, L., "*Aproximación a un Concepto ...", cit.*, nota 35, p. 45-47.

personal, patrimonio o libertad sexual, entre otros) o, incluso, bienes de naturaleza supraindividual (seguridad estatal, paz pública u orden público).

En definitiva, según este criterio, si se produjera el ataque a un sistema informático, además de lesionar el interés particular, se estarían produciendo riesgos para el resto de usuarios.

(ii) Integridad y disponibilidad de los sistemas informáticos.

En este sentido, se parte del archivo y tratamiento informático de datos, la confianza en su autenticidad y en que se podrá disponer de ellos con el empleo de las nuevas tecnologías como bien jurídico protegido. Tal y como veremos en este Capítulo, se ha mantenido que el nuevo artículo 197 *bis* 1 CP lleva a cabo una tutela anticipada de ese bien jurídico.

(iii) Intimidad.

En cuanto al derecho al *habeas data* o autodeterminación informática, tal y como hemos mencionado más arriba, se concibe como el derecho que tienen los ciudadanos a decidir si se difunde su información personal y familiar y en qué forma se difunde. Se trata del poder de control que tiene todo individuo sobre esa información.

En este sentido, HURTADO ADRIÁN[372] ha indicado que los

[372] HURTADO ADRIÁN, A., "Accesos informáticos ilícitos ...", *cit.*, nota

supuestos de *hacking* blanco, aun en los casos que en realidad escondieran un propósito oscuro, quedaban impunes con anterioridad a la citada reforma del año 2010, por cuanto faltaba en ellas el elemento subjetivo de la intencionalidad de atentar contra la intimidad, o su prueba era muy difícil, sin llegar a producirse la vulneración del citado bien que requerían los delitos anteriormente previstos en el artículo 197 CP. Por ello, la modificación del precepto ha supuesto un salto cualitativo, ya que se ha prescindido de las finalidades, incorporando el mero acceso informático sin ningún otro propósito, supuesto que se ha entendido por el legislador como digno de protección penal.

De esta forma, se plantea la cuestión de si la ubicación del nuevo delito es la adecuada o, por el contrario, debió establecerse en un título distinto, en un título de nuevo cuño dedicado exclusivamente a los delitos informáticos o en una ley especial penal especial, tal y como ha sucedido en otros países de nuestro entorno. No obstante, algunos autores han señalado que probablemente la heterogeneidad de bienes jurídicos protegidos es lo que ha motivado que los delitos informáticos no se regulen en un único epígrafe[373].

Mientras el resto de artículos del Título X apenas han recibido modificaciones sustanciales desde que se aprobara el vigente Código penal, el delito de *hacking* ha sido objeto de una nueva reforma con la

---

145, p. 126.

373 ORTS BERENGUER, E. y ROIG TORRES, M., *Delitos informáticos y delitos comunes ...*, *cit*., nota 112, p. 14.

LO 1/2015 tras haber sido incorporado por la LO 5/2010, dando lugar a una nueva ubicación, el artículo 197 *bis*.1 CP. Este nuevo artículo supone la separación de estas conductas de su inicial artículo 197.3 del CP para dar lugar ahora a un delito con un precepto propio que nos permite pensar que su encaje dentro del artículo 197 del CP era un tanto difícil por las especialidades que presenta el *hacking*[374].

El propio legislador es quien ha intentado zanjar la polémica en el apartado XIII del Preámbulo de la LO 1/2015 expuesto más arriba[375], motivando la regulación del *hacking* en un nuevo precepto distinto del anterior artículo 197 por entender que estas conductas,

---

374 En este sentido, el Informe del CGPJ al Anteproyecto de 2006 ya recomendaba la separación de las conductas de *hacking* de las previstas en el artículo 197, por cuanto podía darse el caso en el que el acceso se llevara a cabo sin perjuicio de la intimidad. Así, se establecía: "*el Consejo recomienda que se evite el solapamiento de la nueva figura con las previstas en el artículo 197 CP. En este sentido, el enfoque que da la Decisión Marco a su propuesta armonizadora, que busca de forma directa el aseguramiento de una tutela penal eficiente de la seguridad de los sistemas de información con abstracción de la naturaleza y contenido de los datos comprendidos en los mismos y de la intencionalidad que guíe al culpable, aconseja la ubicación sistemática del nuevo tipo fuera del artículo 197 CP, en un precepto autónomo en el que se sancione la conducta de quien no estando comprendido en ninguno de los supuestos del artículo 197 CP, acceda intencionadamente y sin autorización a un sistema de información ajeno transgrediendo las medidas de seguridad que lo protegen. Una descripción típica de este tenor permitiría cerrar el círculo de protección penal de conductas atentatorias de la intimidad informática, abarcando la incriminación de las conductas de los denominados hacker que en muchas ocasiones se inmiscuyen en sistemas ajenos sin una finalidad específica de perjuicio o de violación de la intimidad, guiados únicamente por el propósito de demostrar su pericia técnica o por un puro afán recreativo*".

375 *Vid*., *supra* subepígrafe 3.1 de este Capítulo.

aunque puedan afectar a la privacidad, no están referidas directamente a la intimidad[376], si bien incluye ese acceso a los sistemas informáticos inmediatamente después de esa disposición, en el artículo 197 *bis* 1, manteniéndolo en el mismo Capítulo que los delitos contra la intimidad con la siguiente redacción:

"*El que por cualquier medio o procedimiento, vulnerando las medidas de seguridad establecidas para impedirlo, y sin estar debidamente autorizado, acceda o facilite a otro el acceso al conjunto o una parte de un sistema de información o se mantenga en él 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*".

Antes de entrar a valorar la certeza o no de esta decisión sistemática, corresponde analizar qué contenido tiene el bien jurídico intimidad.

[376] De conformidad con el apartado XIII de la LO 1/2015: "*De acuerdo con el planteamiento recogido en la Directiva, se introduce una separación nítida entre los supuestos de revelación de datos que afectan directamente a la intimidad personal, y el acceso a otros datos o informaciones que pueden afectar a la privacidad pero que no están referidos directamente a la intimidad personal: no es lo mismo el acceso al listado personal de contactos, que recabar datos relativos a la versión de software empleado o a la situación de los puertos de entrada a un sistema. Por ello, se opta por una tipificación separada y diferenciada del mero acceso a los sistemas informáticos*".

### *3.2.2 Intimidad, secreto, habeas data y propia imagen.*

Tal y como se ha apuntado, los delitos del artículo 197 CP tienen en común la protección de la intimidad, que tiene mayor amplitud que el secreto y que no debe confundirse con éste, por cuanto es entendido como aquello que por su naturaleza o voluntad del titular nadie debe conocer[377], "*lo que una persona o grupo reducido cuidadosamente tiene reservado y oculto*"[378] o "*todo conocimiento reservado, que el sujeto activo no conozca, o no esté seguro de conocer, y que el sujeto pasivo no quiera que conozca*"[379].

Así, autores como ANARTE BORRALLO y DOVAL PAIS[380] han rechazado la inclusión del secreto como bien jurídico protegido, considerando que la protección indiscriminada de los secretos lleva a dotar de una amplitud a los tipos que sería insoportable para el respeto al principio de intervención mínima. En consecuencia, serán típicas las conductas llevadas a cabo para descubrir los secretos relativos a la

---

377 QUERALT JIMÉNEZ, J. J., *Derecho penal español ...*, *cit*., nota 162, p.292.

378 LUZÓN CUESTA, J. M., *Compendio de Derecho Penal. Parte Especial*, ed. Dykinson, Madrid, 2000, p. 91.

379 CARBONELL MATEU, J. C., y GONZÁLEZ CUSSAC, J .L., "Delitos contra la Intimidad ...", *cit*., nota 357, *CD-ROM*.

380 ANARTE BORRALLO, E. y DOVAL PAIS, A., "Delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio (1). Delitos contra la intimidad y los datos personales", en BOIX REIG, J. (Dir.) y VVAA, *Derecho Penal. Parte Especial. Volumen I. La protección penal de los intereses jurídicos personales*, ed. Iustel, segunda edición, Madrid, 2016, pp. 496 y 497.

intimidad de otro o para vulnerar su intimidad, pero no los mismos comportamientos dirigidos al descubrimiento de secretos no referidos a la intimidad. Ello es así por cuanto tal y como venimos manifestando, el bien jurídico protegido es la intimidad y no el secreto al margen de la intimidad. En consecuencia, hay que distinguir entre secretos que afectan a la intimidad de los que no afectan a ese bien jurídico, quedando estos últimos excluidos del ámbito de estas conductas. Este es el criterio que ha mantenido también la Sala segunda del Tribunal Supremo, recordando que el secreto debe estar vinculado a la intimidad, por ser ésta el bien jurídico protegido[381].

También es posible que una situación, que no sea un secreto, esté incorporada en la esfera de intimidad del sujeto y por tanto la conducta de un tercero vulnere la intimidad sin afectar a ningún secreto[382].

---

[381] En este sentido, la STS, Sala Segunda, de 19 de junio de 2006, nº 666/2006, Pte. Excmo. Sr. D. Perfecto Andrés Ibáñez (RJ 2006\4929), FD 4º: "*Así, conforme a lo expuesto, la idea de secreto en el art. 197, 1º CP resulta conceptualmente indisociable de la de intimidad: ese «ámbito propio y reservado frente a la acción y el conocimiento de los demás» (SSTC 73/1982 [RTC 1982, 73] y 57/1994 [RTC 1994, 57] entre muchas)*", citada literalmente también en la STS, Sala Segunda, de 10 de junio de 2011, nº 534/2011, mismo ponente (RJ 2011\4671) o en la STS, Sala Segunda, de 21 de junio de 2016, nº 544/2016, Pte. Excmo. Sr. D. Juan Ramón Berdugo y Gómez de la Torre (RJ 2016\2834).

[382] Así, por ejemplo, la STC 20/1992, Sala Primera, de 14 de febrero de 1992, Recurso 1696/1988, Pte. Excmo. Sr. D. Francisco Tomás y Valiente (RTC 1992\20), consideraba que se había vulnerado la intimidad de una persona por la publicación de su enfermedad en un periódico "*porque en modo alguno puede exigirse a nadie que soporte pasivamente la difusión periodística de datos, reales o supuestos, de su vida privada que afecten a*

Con estas premisas, algunos autores han destacado la dificultad de concretar cuáles son los hechos o informaciones que pertenecen a la intimidad. Aunque deben estar relacionados con la vida privada, esto no significa que se identifiquen con los que se produzcan en el ámbito privado, por cuanto las manifestaciones de la vida privada pueden tener lugar en un espacio público y además en el espacio privado también pueden acontecer hechos que no se incluyan en la esfera de la intimidad. Por ello, ese bien se refiere a la vida privada, manifestada en espacios públicos o privados, como "contexto para sí" donde la persona se desarrolla como ser humano, que es el fin último de su protección, lo que supone excluir los hechos que no afecten a ese contexto íntimo por referirse a otros que se manifiestan con evidente notoriedad o los que se refieren a datos o informaciones que el sujeto opte por extraer de ese ámbito. Esto implica el carácter personalísimo de la intimidad que le faculta para disponer de ella y que no esté reconocida a las personas jurídicas[383].

En cuanto al *habeas data* y el derecho a la propia imagen, se ha apuntado en el subepígrafe anterior cómo se produce una evolución en la esfera de la intimidad del individuo, que comenzaría con un derecho de exclusión físico, con un derecho *to be let alone* a finales del siglo XIX en el que, como indicaban WARREN y BRANDEIS[384],

---

*su reputación, según el sentir común, y que sean triviales o indiferentes para el interés público*".

383 ANARTE BORRALLO, E. y DOVAL PAIS, A., "Delitos contra la intimidad ...", *cit*., nota 380, pp. 497 y 498.

384 WARREN, S. D. y BRANDEIS, L. D., "The right to privacy"..., *cit*., nota

se hacía preciso el reconocimiento de un nuevo ámbito de libertad personal del individuo frente a las intromisiones provocadas especialmente por las fotografías instantáneas y los periódicos a finales del siglo XIX, que ponían en peligro la *privacy* tal y como se entendía hasta esa época, siendo preciso un nuevo ámbito de protección que abarcara ese espacio privado de la vida privada, incluyendo el derecho a la propia imagen. Posteriormente se toma conciencia de los nuevos peligros de la sociedad informatizada tras la Segunda Guerra Mundial, en especial en la década de los años sesenta y el crecimiento de la informática. Como indica MORALES PRATS[385], el derecho a la intimidad debe reciclar su contenido en la sociedad informática, las facultades de exclusión de la esfera privada ya no se encuentran sólo en el ámbito físico, sino que se proyectan también sobre los bancos de datos, el *habeas mentem* que surge con las primeras técnicas de control audiovisual se traduce en *habeas data*, en lo que se entiende, siguiendo a este autor, como la facultad se reconoce al sujeto para "*modular su <<identidad informática>> para que sea veraz y que el reconocimiento de estas facultades sea limitado"*. De esta forma, la evolución del derecho a la intimidad está condicionada por el constante desarrollo tecnológico, lo que no significa que las facultades que se van reconociendo frente a las injerencias tradicionales como el secreto a las comunicaciones o a la propia imagen, se abandonen, sino que se relativizan con las nuevas

362.

385 MORALES PRATS, F., *La tutela penal de la intimidad ..., cit*., nota 363, pp. 43-48.

tecnologías. Por ello, el derecho a la intimidad debe incluir las nuevas relaciones de los sujetos con los sistemas informáticos. Así pues y conforme indica el citado autor, el *habeas data* es el conjunto de derechos que garantiza el control de la identidad informática, que implica el reconocimiento del derecho a conocer, corregir, sustracción o anulación y agregación sobre los datos depositados en un fichero informático[386]. En consecuencia, ese último grupo de facultades configurarían la libertad informática o derecho al control sobre los datos de la propia persona y derivan del principio de acceso a los bancos de datos, dentro del fenómeno de la expansión de la intimidad personal.

Por tanto, siguiendo a ORTS BERENGUER y ROIG TORRES[387], podemos concluir respecto a la intimidad en el ámbito punitivo (i) que los aspectos que la integran son muy variados y en continuo cambio, por lo que no es posible establecer una definición precisa; (ii) que aunque se equipare intimidad y privacidad, o se defina la intimidad de forma limitada, incluyendo tan sólo algunos aspectos de la vida privada, el bien jurídico protegido en los delitos contra la intimidad se debe interpretar restrictivamente, estando integrada por los aspectos más reservados de la persona, conocidos sólo por ella o unas pocas personas, y que no desea que sean divulgados fuera de su círculo limitado; (iii) que las vulneraciones de datos que se refieran a relaciones sociales, sólo constituirán delito contra la intimidad cuando

386 *Ibíd.,* p. 47.

387 ORTS BERENGUER, E. y ROIG TORRES, M., *Delitos informáticos y delitos comunes ..., cit*., nota 112, p. 22.

de su conocimiento resulten elementos relativos a la vida íntima personal o familiar de las personas; y (iv) que las referencias a datos secretos contenidas en los artículos 197 y siguientes se deben relacionar con el bien jurídico protegido en esas normas, por lo que se entenderán reservados los detalles que se refieran a la esfera más estricta de la persona.

### *3.3 El hacking como delito contra la intimidad.*

Atendida la citada evolución histórica del derecho a la intimidad y su contenido actual, se plantea aquí la posibilidad de considerar el delito de intrusismo informático como una de las formas de tutela penal del derecho a la intimidad, con mayor motivo tras la decisión sistemática del legislador con las LO 5/2010 y LO 1/2015.

Así pues, se plantea si la intimidad, entendida en el contexto actual de las nuevas tecnologías y las relaciones de las personas con los sistemas informáticos, constituye el bien jurídico protegido con el delito de *hacking*. Todo ello, como indica MORALES PRATS[388], entendiendo la *privacy* como libertad no limitada a prohibir el uso de la información personal, sino en un sentido positivo hacia el exterior, como derecho de control sobre los datos personales que puedan salir del ámbito íntimo para circular en un banco de datos, es decir, el

[388] MORALES PRATS, F., *La tutela penal de la intimidad ..., cit.*, nota 363, pp. 46-47.

desarrollo del *habeas mentem* a su forma de *habeas data*.

Y ese parece ser el bien jurídico protegido por el legislador del año 2010 si atendemos al criterio sistemático con la introducción del tipo de intrusismo informático en el artículo 197.3 CP con la LO 5/2010, no sólo por tipificar las conductas en el mismo título que los delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio, sino por incluirla dentro del mismo Capítulo que los delitos dedicados al descubrimiento y revelación de secretos y, además, dentro del mismo precepto en el que se tutelan los delitos contra la intimidad. No obstante, como se expone en el Preámbulo de la LO 1/2015:

"*no es lo mismo el acceso al listado personal de contactos, que recabar datos relativos a la versión de software empleado o a la situación de los puertos de entrada a un sistema. Por ello, se opta por una tipificación separada y diferenciada del mero acceso a los sistemas informáticos*"[389].

De esta forma, con esta última modificación el legislador decide regular el *hacking* en un precepto propio, aunque lo hace sin desvincularlo de los delitos contra la intimidad, al mantenerlo en el mismo Capítulo, lo que plantea el problema que el propio legislador apunta en el Preámbulo, por cuanto no es lo mismo la entrada a un sistema informático desvinculado de relación alguna con el citado derecho, que el acceso a datos sensibles o de cualquier otra forma

[389] Preámbulo de la LO 1/2015, apartado XIII.

ligados a la esfera de la intimidad de las personas. Como indica MUÑOZ CONDE, se produce una separación entre las conductas del descubrimiento o revelación de datos que atentan contra la intimidad personal y el acceso no autorizado a otras informaciones que, aunque puedan afectar a la privacidad, no están referidos directamente a la intimidad personal[390].

Precisamente esta decisión del legislador con sus dos reformas ha supuesto numerosas críticas que se exponen en el siguiente subepígrafe.

### *3.4 Críticas a la consideración del delito de hacking como un delito contra la intimidad.*

Como se ha anticipado en el punto anterior, la ubicación de las nuevas conductas entre los delitos contra la intimidad ha suscitado cierta polémica entre la doctrina por no considerar la intimidad como el bien jurídico protegido en el nuevo tipo del artículo 197 *bis* 1 del CP.

En este sentido, fueron numerosas las voces críticas por la ubicación sistemática del delito de *hacking* en el artículo 197 del CP con la reforma llevada a cabo con la LO 5/2010[391], por cuanto en

390 MUÑOZ CONDE, F., *Derecho penal. Parte especial*, ed. Tirant lo Blanch, Valencia, 2015, p. 240.

391 Entre otros, DE LA MATA BARRANCO, N. J. y HERNÁNDEZ DÍAZ, L.,

realidad con el delito se trata de proteger la privacidad en la utilización del sistema informático, no la intimidad, mientras que en el precepto se tutela la intimidad en sus dos vertientes: (i) la vertiente clásica o negativa consistente en el derecho a excluir a terceros que correspondería con el apartado 1; y (ii) la vertiente más reciente que comprende un derecho a controlar los datos propios correspondiente a su apartado 2.

El nuevo artículo 197 *bis* 1 del CP introducido por la LO 1/2015, anterior artículo 197.3, lejos de aportar claridad en torno al bien jurídico protegido con el delito de intrusismo informático, separándolo de los delitos contra la intimidad, se ha seguido manteniendo en el mismo Título, siendo catalogado además de excesivamente casuístico y enrevesado[392].

En esta línea crítica también se pronuncia MORALES PRATS. Después de exponer el acierto sistemático del Código de 1995 en lo que respecta a la creación de un Título específico para los delitos contra la intimidad, el autor critica que la rúbrica acoja no sólo la intimidad, sino también el derecho a la propia imagen y la inviolabilidad del domicilio. La inclusión del delito de *hacking* con la reforma de 2010 también merece el reproche de este autor, pues no

---

por considerar que lo que en realidad se trata de proteger no es la intimidad, sino la privacidad en la utilización del sistema informático. *Vid.,* "Los delitos vinculados a la informática en el Derecho penal español", en DE LA CUESTA ARZAMENDI, J. L. (Dir.) y VVAA, *Derecho Penal Informático, ed. Civitas, Pamplona, 2010*, p. 159.

392 TOMÁS-VALIENTE LANUZA, C., "Título X. Delitos contra la Intimidad ...", *cit*., nota 127, p. 794.

existe criterio sistemático alguno y se desprecia el bien jurídico por el que se optó en 1995, hasta tal punto de "enchuletar" el nuevo delito en el artículo 197 CP, con los consiguientes problemas interpretativos y el corrimiento de la numeración dentro del precepto. Así, según expone, por una parte, el precepto no se refiere a datos o programas informáticos que contengan datos personales y, por otra, el citado delito constituye una barrera previa de tutela de otros bienes distintos a la intimidad, como pueden ser los secretos empresariales o el patrimonio, siempre que se proyecten sobre los datos o programas informáticos. Por ello, el grave error sistemático del legislador con la reforma de 2010 se habría evitado con un Título específico para el acceso ilícito a los sistemas informáticos, desanclando los delitos informáticos del principio de lesividad y de la identificación clara de los bienes jurídicos que se protejan, o al menos un capítulo propio para evitar los problemas interpretativos[393]. Por su parte, la reforma del año 2015 perjudica la claridad sistemática que contenían los tipos penales en el Código de 1995 y con ella el legislador ha dejado pasar la oportunidad de mejorar técnicamente el texto originario en cuanto a los delitos contra la intimidad[394].

En esta línea, COLÁS TURÉGANO cuestiona el mantenimiento de la rúbrica del título, referida a la intimidad, y que tal vez se debería haber reflexionado la creación de un título propio

[393] MORALES PRATS, F., "Título X. Delitos contra la intimidad …", *cit*., nota 369, pp. 451, 481 y 482.

[394] MORALES PRATS, F., "La reforma de los delitos contra la intimidad ...", *cit*., nota 167, p. 459 y 460.

donde incluir los delitos de nueva creación a los que nos estamos refiriendo[395].

Aunque entendamos que con el acceso no autorizado a un sistema informático se pueda alcanzar información personal y se pueda afectar a la intimidad, se ha considerado un acierto que al menos se haya separado el delito de *hacking* de las conductas del artículo 197 CP, pasando del artículo 197.3 del CP introducido por la LO 5/2010 al nuevo artículo 197 *bis* 1 tras la LO 1/2015, a pesar que no se haya creado un título, capítulo o sección propia para este tipo de conductas. En este sentido se ha pronunciado CASTELLÓ NICÁS, quien ha defendido que en este delito el secreto de una persona puede ser intrascendente, pues lo que interesa es obtener información por un interés presente o futuro[396].

Por su parte, JORGE BARREIRO[397] critica que si el bien jurídico protegido en el artículo 197 *bis* 1 fuera la intimidad, quedarían fuera de estas conductas los accesos ilícitos a sistemas informáticos públicos y también señala la menor pena prevista en relación con las conductas de los apartados 1 y 2, que regulan propiamente los delitos contra la intimidad, lo que supone un

---

395 COLÁS TURÉGANO, A., "Nuevas conductas delictivas ...", *cit*., nota 168, p. 663.

396 CASTELLÓ NICÁS, N., "Delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio, y delitos contra el honor", en MORILLAS CUEVA, L. (Dir.) y VVAA, *Estudios sobre el Código penal reformado*, ed. Dykinson, Madrid, 2015, p. 506.

397 JORGE BARREIRO, A., "Delitos contra la intimidad ...", *cit*., nota 117, p. 1043.

tratamiento punitivo separado de los ataques contra la intimidad en sentido estricto.

Así pues, si la intimidad constituyera el bien jurídico protegido en el nuevo artículo 197 *bis* 1 del CP, en el sentido de que pudiera pensarse que los datos o programas deben albergar información relevante para la intimidad personal o familiar, plantearía problemas de delimitación con el artículo 197.2[398] y supondría la atipicidad de las conductas que precisamente parecen querer tutelarse, como sería el acceso a sistemas informáticos de la Administración Pública que no incluyesen información íntima, pero que recogiesen cualquier otro tipo de información. A esta interpretación se añade la menor gravedad de la pena respecto a los apartados 1 y 2[399], razón por la cual TOMÁS-VALIENTE LANUZA considera que el bien jurídico protegido es instrumental y no está vinculado a la intimidad[400].

---

398 Este artículo establece las mismas penas que el artículo 197.1 del CP "*al que, sin estar autorizado, se apodere, utilice o modifique, en perjuicio de tercero, datos reservados de carácter personal o familiar de otro que se hallen registrados en ficheros o soportes informáticos, electrónicos o telemáticos, o en cualquier otro tipo de archivo o registro público o privado. Iguales penas se impondrán a quien, sin estar autorizado, acceda por cualquier medio a los mismos y a quien los altere o utilice en perjuicio del titular de los datos o de un tercero*".

399 Los tipos básicos de los apartados 1 y 2 del artículo 197 del CP conllevan penas de prisión de uno a cuatro años y multa de doce a veinticuatro meses, frente a la pena de prisión de seis meses a dos años prevista para el delito de *hacking* en el artículo 197 *bis*.1 del CP.

400 TOMÁS-VALIENTE LANUZA, C., "Título X. Delitos contra la Intimidad ...", *cit*., nota 126, pp. 802 y 803.

Para HURTADO ADRIÁN[401] la tipificación del acceso ilícito a los sistemas informáticos supone un salto cualitativo porque se prescinde de algún otro propósito, pero a su vez, si se prescinde del ataque a la intimidad, no deberían haberse incluido estas conductas junto a los delitos caracterizados por esos ataques, aunque la denominada dinámica externa del delito sea coincidente con la del artículo 197.2 CP. Por ello, si con el delito previsto en el artículo 197.2 CP se tutela la *privacy i*nformática o *habeas data* y con la reforma de 2010 se protegen los sistemas de información en el artículo 197.3 CP, resulta criticable la ubicación sistemática de este último precepto.

Por su parte, la jurisprudencia[402] ha destacado la necesaria

---

401 HURTADO ADRIÁN, A., "Accesos informáticos ilícitos ...", *cit*., nota 145, pp. 126 y 127.

402 Así, la STS de 24 de febrero de 2015, *cit*., nota 83, con ocasión de los delitos de corrupción y prostitución de menores y "grooming", declara en su FD 4º que "*Es evidente que cuando su titular navega por Internet, participa en foros de conversación o redes sociales, descarga archivos o documentos, realiza operaciones de comercio electrónico, forma parte de grupos de noticias, entre otras posibilidades, está revelando datos acerca de su personalidad, que pueden afectar al núcleo más profundo de su intimidad por referirse a ideologías, creencias religiosas, aficiones personales, información sobre la salud, orientaciones sexuales, etc. Quizás, estos datos que se reflejan en un ordenador personal puedan tacharse de irrelevantes o livianos si se consideran aisladamente, pero si se analizan en su conjunto, una vez convenientemente entremezclados, no cabe duda que configuran todos ellos un perfil altamente descriptivo de la personalidad de su titular, que es preciso proteger frente a la intromisión de terceros o de los poderes públicos, por cuanto atañen, en definitiva, a la misma peculiaridad o individualidad de la persona. A esto debe añadirse que el ordenador es un instrumento útil para la emisión o recepción de correos electrónicos,*

protección de la intimidad en la regulación de los accesos ilícitos a los sistemas informáticos, por cuanto aunque los datos contenidos en esos sistemas puedan considerarse irrelevantes aisladamente, en su conjunto pueden configurar una descripción detallada de la personalidad de su titular, afectando la intimidad, a lo que se añade la emisión, recepción y almacenamiento de correos electrónicos en los sistemas informáticos que implican la afectación al derecho al secreto de las comunicaciones, lo cual requiere su protección frente a las conductas de *hacking*. Por ello, tanto desde la perspectiva del derecho de exclusión del propio entorno virtual, como de las garantías constitucionales exigidas para el sacrificio de los derechos a la inviolabilidad de las comunicaciones y a la intimidad, la intervención de un ordenador para acceder a su contenido exige un acto jurisdiccional habilitante[403].

---

*pudiendo quedar afectado en tal caso, no sólo el derecho al secreto de las comunicaciones del art. 18.3 CE (por cuanto es indudable que la utilización de este procedimiento supone un acto de comunicación), sino también el derecho a la intimidad personal (art. 18.1 CE), en la medida en que estos correos o email, escritos o ya leídos por su destinatario, quedan almacenados en la memoria del terminal informático utilizado. Por ello deviene necesario establecer una serie de garantías frente a los riesgos que existen para los derechos y libertades públicas, en particular la intimidad personal, a causa del uso indebido de la informática así como de las nuevas tecnologías de la información*".

[403] En este sentido, la citada STS de 24 de febrero de 2015 matiza que "*esa autorización no está incluida en la resolución judicial previa para acceder al domicilio en el que aquellos dispositivos se encuentran instalados. De ahí que, ya sea en la misma resolución, ya en otra formalmente diferenciada, el órgano jurisdiccional ha de exteriorizar en su razonamiento que ha tomado en consideración la necesidad de sacrificar,*

Por otra parte, considerando la dificultad para determinar qué hechos, datos, imágenes o informaciones pertenecen a la intimidad, ANARTE BORRALLO y DOVAL PAÍS[404] destacan que la interpretación de las nuevas conductas dentro de la órbita de la intimidad supone numerosos problemas, entre los que destacan los siguientes:

(i) sus elementos no se refieren expresamente a la intimidad;

(ii) si se considera como bien jurídico la seguridad de los sistemas de información, tal y como veremos en el siguiente apartado, supone un adelantamiento de la intervención penal y la cuestión de la legitimidad de la intervención penal; y

(iii) en las normas comunitarias se descarta la intimidad como bien jurídico protegido.

Por ello, parece que el legislador ha intentado disimular estas carencias no regulando los nuevos delitos en un lugar propio del Código y se puede aventurar una cierta incongruencia en los tribunales cuando apliquen los nuevos preceptos, ubicados entre los delitos contra la intimidad, a casos en los que fundamentalmente se afecta a intereses mercantiles, institucionales o políticos.

---

*además del domicilio como sede física en el que se ejercen los derechos individuales más elementales, aquellos otros derechos que convergen en el momento de la utilización de las nuevas tecnologías*". *Ibíd*., FD 4º.

[404] ANARTE BORRALLO, E. y DOVAL PAIS, A. "Delitos contra la intimidad ...", *cit*., nota 380, pp. 497 y 498, 511-513.

Todo ello nos lleva a plantearnos si el nuevo delito de *hacking* debería haberse ubicado en un nuevo título del Código Penal junto a otros delitos relacionados con la informática como el delito de daños informáticos introducido en el artículo 264 del CP tras la reforma de la LO 5/2010[405], obstaculizar o interrumpir el funcionamiento de sistemas informáticos previsto en el artículo 264 *bis*, producir, adquirir, importar o facilitar programas para cometer esos delitos, previsto en el artículo 264 *ter*, o cuando es una persona jurídica quien comete estos delitos, previsto en el artículo 264 *quater*[406]. Desde mi punto de vista, la separación entre los delitos contra la intimidad y los delitos de acceso a un sistema informático, tipificado en un título autónomo, habría facilitado la interpretación del precepto y una mejor solución a su concurso con otros hipotéticos delitos.

### *3.5 La seguridad de los sistemas informáticos como bien jurídico protegido*.

El planteamiento del bien jurídico protegido en el caso de estas conductas condiciona el enfoque de problemas tales como la exigencia o no de una finalidad jurídica añadida a la simple curiosidad o

[405] Tras la LO 5/2010, el delito de daños informáticos deja de ser un subtipo agravado para tipificarse como un delito autónomo en el artículo 264 del CP.

[406] Los artículos 264 *bis*, 264 *ter* y 264 *quater* del CP han sido introducidos por la reforma llevada a cabo con la LO 1/2015.

demostración de pericia informática que pueda tener un *hacker* y si resulta necesario o no adelantar la barrera de intervención del Derecho penal para tipificar estas conductas como un delito autónomo[407].

Como hemos visto, la ubicación sistemática del artículo 197 *bis* 1, y en mayor medida su ubicación anterior en el artículo 197.3, puede inducirnos a entender como bien jurídico protegido la intimidad[408]. Sin embargo, citando el Preámbulo del Convenio Europeo sobre Cibercriminalidad[409], a raíz de la reforma de la LO 5/2010 autores como RUEDA MARTÍN[410] han defendido la existencia de un nuevo bien jurídico, objeto de lesión o puesta en peligro con estos delitos: la confidencialidad, integridad y disponibilidad de los datos y sistemas informáticos.

Así, según esta autora, la *integridad* se refiere a la posible utilización del sistema, con las pertinentes modificaciones del contenido de la información almacenada en el sistema, por la persona autorizada; la *confidencialidad* se basa en la utilización del sistema sólo por la persona autorizada; y, por último, la *disponibilidad* hace

---

407 En este sentido, RUEDA MARTÍN, M. Á., "Los ataques contra los sistemas informáticos ...", *cit*., nota 347, p. 362.

408 QUERALT JIMÉNEZ, J. J., *Derecho Penal Español ...*, *cit*., nota 162, pp. 283-284.

409 En su Preámbulo se dice: "*el presente Convenio es necesario para prevenir los actos atentatorios de la confidencialidad, la integridad y la disponibilidad de los sistemas informáticos, de las redes y de los datos, así como el uso fraudulento de tales sistemas, redes y datos, asegurando la incriminación de dichos comportamientos, como los descritos en el presente Convenio*".

410 RUEDA MARTÍN, M. Á., "Los ataques contra los sistemas informáticos ...", *cit*., nota 347, p. 364.

referencia al control sobre la utilización de un sistema por parte de la persona autorizada. Según este criterio, la consideración de la confidencialidad, integridad y disponibilidad de los sistemas informáticos como bien jurídico protegido justifica la represión penal autónoma de las conductas de *hacking* por varias razones:

1) por el interés en la seguridad de la utilización de las TIC, sirviendo ese bien jurídico como barrera de contención para otros bienes jurídicos;

2) por la armonización legislativa con el derecho comparado y comunitario; y

3) porque la informática es una fuente de peligro que necesita un control y, por sus repercusiones sobre otros bienes jurídicos, está legitimada la intervención del Derecho penal.

Se trataría por tanto de un bien jurídico distinto a la intimidad, que no excluiría también su tutela, por cuanto considerar que la confidencialidad, la integridad y la disponibilidad de los sistemas informáticos constituye el bien jurídico protegido, supone la tutela frente a riesgos para otros bienes jurídicos que puedan estar involucrados en la función de los sistemas y redes informáticas, como puede ser la intimidad o el patrimonio. Dicho en otras palabras, la protección de estos últimos bienes jurídicos será mayor en la medida que se garantice la confidencialidad, la integridad y la disponibilidad de los sistemas informáticos en los que se involucren. Este bien

jurídico actúa como barrera de "contención de riesgos"[411] para otros bienes jurídicos. Como indica HURTADO ADRIÁN, en la protección del sistema de información se encuentra la esencia del bien jurídico a proteger[412].

Este es el criterio que parece seguir el legislador europeo con la DM 2005/222/JAI al referirse expresamente a la protección de los sistemas de información en sus considerandos 1 y 2[413] o en el Considerando 26 de la Directiva 2013/40/UE, donde impone a los Estados miembros la adopción de medidas para proteger "*los sistemas de información*"[414], por lo que este legislador parece inclinarse porque el bien jurídico protegido vendría constituido por la seguridad de los

---

411 *Ibíd*., p. 370.

412 HURTADO ADRIÁN, A., "Accesos informáticos ilícitos ...", *cit*., nota 145, p. 129.

413 Los considerandos 1 y 2 de la DM establecen: "*1) El objeto de la presente Decisión marco es reforzar la cooperación entre las autoridades judiciales y otras autoridades competentes, incluida la policía y los demás servicios represivos especializados de los Estados miembros, mediante la aproximación de su legislación penal en materia de ataques contra los sistemas de información. (2) 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. 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*".

414 Según dispone el Considerando 26 de la Directiva, "*Para combatir eficazmente la ciberdelincuencia, debe aumentarse la capacidad de adaptación de los sistemas de información mediante la adopción de las medidas adecuadas para protegerlos de manera más eficaz contra los ataques que les afecten*".

sistemas informáticos o, de forma más genérica, los sistemas de información (sistemas informáticos en términos clásicos), tal y como señalan ANARTE BORRALLO y DOVAL PAÍS, o su buen funcionamiento y seguridad[415].

Este planteamiento del legislador europeo implica carencias en la legitimidad de la intervención penal, en cuanto a la determinabilidad del objeto protegido y medio de ataque y por tanto la seguridad jurídica, la subsidiariedad, intervención mínima y la proporcionalidad y quizás para disimularlas el legislador español ha optado por no incluir estos nuevos delitos en un capítulo propio, tratando de resguardar la legitimidad de la intervención penal al cumplir con la normativa comunitaria[416].

En esta línea, con la reforma de la LO 5/2010, HURTADO ADRIÁN[417] ha señalado que con este delito se tutelan los sistemas de información, citando el punto 8 del Informe de la Comisión de estudios e informes del CGPJ emitido en fecha 18 de febrero de 2009, al Anteproyecto de LO por la que se modifica el CP[418] y la DM

---

415 ANARTE BORRALLO, E. y DOVAL PAIS, A., "Delitos contra la intimidad ...", *cit*., nota 380, p. 512.

416 *Ibíd*., p. 512.

417 HURTADO ADRIÁN, A., "Accesos informáticos ilícitos ...", *cit*., nota 145, p. 127.

418 El punto 8 del citado Informe dice que "*el bien jurídico protegido no es la intimidad, sino la integridad y la indemnidad del propio sistema que protege los datos. Tal y como ha propuesto la doctrina, la conducta típica afecta a la seguridad colectiva del tráfico informatizado*". Informe de la Comisión de estudios e informes del CGPJ emitido en fecha 18 de febrero de 2009, al Anteproyecto de LO por la que se modifica el CP, disponible en

2005/222/JAI, Considerando 2[419], Considerando 3[420] y Considerando 14[421]. En consecuencia, entiende que se protege un nuevo bien jurídico, la seguridad informática dentro del marco de la confidencialidad del sistema informático, lo que supone un adelantamiento de las barreras de protección en relación con eventuales ataques a otros bienes jurídicos individuales que pudieran verse afectados por el acceso ilícito al sistema de información.

También NÚÑEZ CASTAÑO ha entendido tutelada la seguridad de las redes y de los sistemas informáticos[422], que según indican CARBONELL MATEU y GONZÁLEZ CUSSAC son indispensables para garantizar la integridad, confidencialidad y disponibilidad de los datos que almacenan o transmiten[423]. Se trata, según este último grupo de autores, de proteger la seguridad de los sistemas informáticos[424], que afectan a la seguridad del tráfico informatizado, por lo que de nuevo se critica su desafortunada

---

http://www.aelpa.org/actualidad/julio2009/Informa%20CP-%20CGPJ.doc, consultado el 4 de octubre de 2016.

419 *Vid*., nota 413.

420 El Considerando 3 dispone: "*Para responder con eficacia a esas amenazas es necesario un planteamiento global en materia de seguridad de las redes y de la información*".

421 Según se dice en el Considerando 14, "*Es necesario que los Estados miembros prevean sanciones para reprimir los ataques contra los sistemas de información*". DM 2005/222/JAI, *cit.*, nota 95.

422 NUÑEZ CASTAÑO, E. "Lección XII. Delitos contra la intimidad ...", *cit*., nota 351, p. 230.

423 CARBONELL MATEU, J.C. y GONZÁLEZ CUSSAC, J. L., "Delitos contra la Intimidad ...", *cit*., nota 357, *CD-ROM*.

424 En este sentido también, ANARTE BORRALLO, E. y DOVAL PAIS, A., "Delitos contra la intimidad ...", *cit*., nota 166, p. 455.

ubicación, pues los datos o programas informáticos en ocasiones no tendrán relación alguna con la intimidad. La seguridad de los sistemas como bien jurídico también se ha mantenido por otros autores como CARRASCO ANDRINO[425], CASTELLÓ NICÁS[426] o COLÁS TURÉGANO, quien destaca el énfasis del apartado XIII del Preámbulo de la LO 1/2015[427] hacia la tutela de la seguridad de los sistemas informáticos, frente a la tutela de la intimidad. Esto supone para esta última autora su configuración como delito de peligro abstracto para la seguridad de las redes informáticas, tal y como veremos en el epígrafe 5[428].

No obstante, MUÑOZ CONDE ha defendido que aunque se tutele directamente la seguridad de los datos y sistemas informáticos, dentro de ella también se protegen la intimidad y los datos que pueden encontrarse dentro del sistema[429].

Como señalan ANARTE BORRALLO y DOVAL PAÍS[430], la consecuencia del planteamiento de los sistemas de información, o su

---

425 CARRASCO ANDRINO, M. M., "El Delito de Acceso Ilícito a los Sistemas Informáticos", en ÁLVAREZ GARCÍA, F.J., GONZÁLEZ CUSSAC, J. L. (Dir.) y VVAA, *Comentarios a la Reforma Penal de 2010,* ed. Tirant Lo Blanch, Valencia, 2010, p. 249.

426 CASTELLÓ NICÁS, N., "Delitos contra la intimidad ...", *cit*., nota 396, p. 505.

427 Respecto al apartado XIII del Preámbulo de la LO 1/2015, *vid*., subepígrafe 3.1 de ese Capítulo.

428 COLÁS TURÉGANO, A., "Nuevas conductas delictivas ...", *cit*., nota 168, pp. 673 y 677.

429 MUÑOZ CONDE, F., *Derecho penal ...*, *cit*., nota 109, p. 277.

430 ANARTE BORRALLO, E. y DOVAL PAIS, A., "Delitos contra la intimidad ...", *cit*., nota 380, p. 513.

buen funcionamiento y seguridad, como bien jurídico protegido es que posiblemente los órganos jurisdiccionales sigan aplicando estos preceptos a escasos supuestos, resistiéndose a aplicarlos salvo en los casos en que esté en juego la intimidad, atendido el Capítulo en el que se encuentran. Los tribunales también van a encontrarse con un desfase entre los fundamentos legitimadores de estos nuevos delitos, expuestos en la Directiva 2013/40/UE y la realidad. Su Considerando 3 establece:

"*Los ataques contra los sistemas de información y, en particular, los ataques vinculados a la delincuencia organizada, son una amenaza creciente en la Unión y en el resto del mundo, y cada vez preocupa más la posibilidad de ataques terroristas o de naturaleza política contra los sistemas de información que forman parte de las infraestructuras críticas de los Estados miembros y de la Unión*". Lo que supone un fundamento referido a la delincuencia organizada, que ignora que en realidad el intrusismo informático es un fenómeno que crece al ritmo acelerado de las nuevas tecnologías y no sólo vinculado a la delincuencia organizada, tal y como veremos en el siguiente Capítulo.

Y, por último, es previsible una incongruencia entre el delito de *hacking* que se ubica entre los delitos contra la intimidad y la aplicación a casos donde primarán los intereses empresariales, institucionales o políticos.

En consecuencia, según estos autores, resulta necesaria una interpretación sistemática del artículo 197 *bis* 1, considerándolo un

medio de protección anticipada de la intimidad para lograr una cierta coherencia. Esto supone entenderlo como un delito de peligro donde la relación de los presupuestos de responsabilidad con ese bien jurídico se centran en que el objeto sobre el que recaiga la conducta debe tener capacidad para representarla y en el objeto del dolo del sujeto.

Por otra parte, tras la reforma de la LO 5/2010 también se ha dicho que el legislador, al igual que en el delito de allanamiento de morada, ha presumido el vínculo entre el acceso no consentido con la intimidad en la simple realización de la conducta base. Esa vinculación se evidencia por la ubicación sistemática del precepto, resultando así la voluntad del legislador de ligar el delito a la intimidad personal. En estos casos MORALES GARCÍA ha venido hablando de la tutela del citado domicilio informático[431]. El domicilio informático vendría a ser el derecho a mantener los espacios de actuación en red y su contenido al margen de los accesos no deseados, en equivalencia a lo que sucede con el domicilio físico. Lo que ocurre es que el espacio informático no lo configura una máquina, sino la información situada en ese espacio. Para este autor la legitimación del delito no ligado a un elemento subjetivo del injusto es expresión de la evolución de estas conductas que se refieren en su descripción objetiva al ataque a un bien jurídico que necesitaba de otras referencias para su identificación, por cuanto los elementos subjetivos

[431] MORALES GARCÍA, O., "Delincuencia informática ...", *cit*., nota 142, pp. 185 y 186.

del injusto no permitían constatar la relevancia del espacio informático para la intimidad. De esta forma, también destaca la mención al mantenimiento en el sistema contra la voluntad de quien tenga el legítimo derecho a excluirlo, por cuanto se ubica al domicilio informático en un plano similar al domicilio físico. Postura que también sustenta en el Derecho italiano, donde desde la Sentencia 1675/2000 de la Corte Suprema de Casación se ha hecho referencia al citado domicilio informático como objeto instrumental de tutela:

"*Non si tratta perciò di un illecito caratterizzato dal l'effrazione dei sistemi protettivi, perché altrimenti non avrebbe rilevanza la condotta di chi, dopo essere legittimamente entrato nel sistema informatico, vi si mantenga contro la volontà del titolare. Ma si tratta di un illecito caratterizzato appunto dalla contravvenzione alle disposizioni del titolare, come avviene nel delitto di violazione di domicilio, che è stato notoriamente il modello di questa nuova fattispecie penale, tanto da indurre molti a individuarvi, talora anche criticamente, la tutela di un "domicilio informatico"*[432].

Esta Sentencia se refiere a que el delito de *hacking* no se caracteriza por vulnerar el sistema de protección, por cuanto entonces no tendría relevancia la conducta del que, entrando legalmente, se mantiene en el sistema contra la voluntad del titular, sino que se caracteriza por contravenir lo dispuesto por su titular, como en los

[432] Motivo 2 de la Sentencia 1675/2000 de la Corte Suprema de Casación italiana, Sección Quinta, de fecha 7 de noviembre de 2000. El texto íntegro está disponible en http://www.penale.it/giuris/cass_011.htm, consultado el 4 de octubre de 2016.

delitos de allanamiento de morada, que es el modelo de este nuevo delito, identificándose la protección del domicilio informático.

Así, también con referencia al artículo 615 *ter* del Código Penal italiano[433], PECORELLA[434] se refiere al domicilio informático según el modelo del delito de violación del domicilio previsto en el artículo 614 del Código italiano.

Según esta idea, la citada comparación con el lugar donde el sujeto con derecho a ello desarrolla su vida privada es parcial. Y ello porque el precepto también es aplicable a sistemas informáticos de interés público y, además, al exigirse la vulneración de medidas de seguridad, protegiendo sólo los sistemas de información que dispongan de esas medidas, esa exigencia resultaría injustificada si lo que se pretende es que el ordenador sea un nuevo domicilio protegido como el domicilio tradicional. En consecuencia, la naturaleza del delito no estaría clara, pudiéndose entender como un delito de daño contra el denominado domicilio informático, o bien como un delito de peligro contra los datos contenidos en el sistema. En este último caso, cabría entenderlo como un peligro para la integridad de los datos, acorde con la previsión de la agravante del mismo artículo cuando el peligro se traduzca en daño, o como un riesgo para su confidencialidad, acorde con la experiencia criminológica y la

433 *Vid., supra* subepígrafe 4.11 del Capítulo II.

434 PECORELLA, C., "El acceso abusivo a los sistemas informáticos o telemáticos", en ANARTE BORRALO, E., MORENO MORENO, F. y GARCÍA RÚIZ, C. (Coordinadores), *Nuevos conflictos sociales. El papel de la privacidad*, ed. Iustel, Madrid, 2015, p. 270.

fundamentación expuesta en la normativa internacional[435]. La consideración de un delito de peligro para la confidencialidad conlleva tener en cuenta el carácter residual del delito de *hacking* en el ordenamiento italiano, al estar tipificada prácticamente cualquier agresión contra datos y programas, concluyendo esta autora con la idea de que el tipo tiene necesariamente la función de castigar anticipadamente los hechos de espionaje informático. No sería posible una función propia para el fraude y daños informáticos, por cuanto respecto a las normas que ya castigan estas conductas, supondría anticipar la intervención penal sin justificación por cuanto se sanciona el acceso abusivo sin considerar la función y tipo de datos que se contienen. A la naturaleza juríidca del delito de *hacking*, se dedica el epígrafe 5 de este Capítulo.

En esta última línea se ha dictado alguna resolución que en aplicación del artículo 197.3, en su redacción dada por la LO 5/2010, ha manifestado que el bien jurídico protegido es la libertad informática o domicilio informático, siendo irrelevantes los datos contenidos en el sistema informático[436].

---

435 Así, según el Considerando 6 de la Directiva 2013/40/UE, "*Los ciberataques a gran escala pueden causar graves perjuicios económicos, tanto por la paralización de los sistemas de información y de las comunicaciones como por la pérdida o alteración de información confidencial de importancia comercial o de otros datos*".

436 En este sentido, en un supuesto en el que el acusado había realizado tres intentos fallidos de acceso al panel de control de Internet protegido por contraseña y sin autorización de su titular, razón por la cual fue condenado por el delito del anterior artículo 197.3 en grado de

Siguiendo estas últimas teorías, las medidas de seguridad quebrantadas son el medio por el que el sujeto pasivo establece la vinculación de sus datos o programas con esferas de reserva, por tanto las medidas de seguridad que el sujeto establece permiten seleccionar y fijar cuáles son los ataques más vinculados al bien jurídico protegido, que a través del domicilio informático termina siendo la intimidad.

En este sentido, para MORALES GARCÍA la inclusión en el anterior artículo 197.3 de las conductas de mantenimiento en el sistema informático, en el mismo precepto que el *hacking*, conductas que se han mantenido en el nuevo artículo 197 *bis* 1, vendría a situar el domicilio informático en un plano de tutela similar al de la tutela del domicilio físico[437].

Por su parte, partiendo del rechazo a la ubicación sistemática del precepto, MORALES PRATS[438], en línea con CARRASCO

---

tentativa "*al no haber logrado el acusado con la contraseña utilizada acceder al programa informático*", la SAP de Vizcaya nº 90307/2014, de 23 julio, Sección 2ª, Recurso de Apelación núm. 143/2014, Pte. Ilmo. Sr. D. Manuel Ayo Fernández (JUR 2014\267848), declara en su FD 4º: "*siendo este delito el denominado de intromisión informática en que lo se protege es la libertad informática o más exactamente el domicilio informático de una persona, no siendo relevante la naturaleza de los datos contenidos en el sistema informático pudiendo ser de naturaleza personal, familiar, económicos o de otra índole que pertenezcan al ámbito privado de dicha persona.*".

[437] MORALES GARCÍA, O., "Comentario a los delitos informáticos de los arts. 197, 248 y 264 CP", en VVAA, *Delincuencia informática. Tiempos de cautela y amparo*, ed. Aranzadi, primera edición, Navarra, 2012, p. 154.

[438] MORALES PRATS, F., "Título X. Delitos contra la intimidad ...", *cit*.,

ANDRINO, se ha referido a la seguridad de las redes y sistemas informáticos como bien jurídico protegido, por ser el que deriva de los instrumentos internacionales (DM 2005/222/JAI y Convenio sobre Cibercriminalidad). En todo caso, atendiendo a la ubicación del entonces artículo 197.3 CP entre los delitos contra la intimidad y, citando la idea de MORALES GARCÍA sobre la inviolabilidad del domicilio informático[439], señala que esta propuesta conlleva la de seguridad, por cuanto tradicionalmente el domicilio ha estado vinculado a la seguridad personal. Por ello, esta hipótesis que fija en el domicilio informático el bien jurídico no es incompatible con la seguridad de las redes y sistemas de información como objeto de tutela. En consecuencia, como resultado de su ubicación sistemática, el acceso ilícito deberá proyectarse en conductas que potencialmente sean susceptibles de afectar a la intimidad personal. El delito protege la seguridad de los sistemas informáticos, pero con el fin último de tutelar la *privacy* informática de las personas.

En este sentido, JORGE BARREIRO también entiende que la seguridad informática se configura como bien jurídico tutelado. La define como la seguridad de datos y sistemas informáticos, en la medida que la tutela a la intimidad dejaría excluidos los ataques a sistemas informáticos públicos y no explicaría el tratamiento separado de estas conductas respecto a las que tutelan la intimidad en sentido estricto. Todo ello, sin olvidar que con la tutela de la seguridad

---

nota 369, p. 482.

439 MORALES GARCÍA, O., "Delincuencia informática ...", *cit*., nota 142, pp. 185 y 186.

informática se trata de proteger también la intimidad integrada en el sistema informático[440].

Desde mi punto de vista, conforme a estos últimos plantemientos, tal y como se explicará en el epígrafe 6, la seguridad de los sistemas informáticos, que comprende la confidencialidad, integridad y disponibilidad de ese sistema, es el bien jurídico protegido por el artículo 197 *bis* 1 de forma directa, sin olvidar que esto supone la protección indirecta de otros derechos, donde también se comprendería la intimidad, pero no necesariamente ésta. Dicho en otras palabras, la protección de la seguridad de los sistemas informáticos implica el adelantamiento de las barreras de tutela que supone la tipificación del mero acceso al sistema informático, protegiendo indirectamente cualquier otro bien jurídico que con el acceso y la puesta en peligro de la seguridad del sistema pudiera verse afectado, tanto la citada intimidad, como el patrimonio, la propiedad, el secreto de empresa u otro bien jurídico protegido, cuya efectiva lesión o puesta en peligro dará lugar al correspondiente concurso, a los que se hace referencia en el siguiente Capítulo, epígrafe 5.

### *4. EL OBJETO MATERIAL.*

Como objeto de la acción se refería MEZGER a aquel objeto

[440] JORGE BARREIRO, A., "Delitos contra la intimidad ...", *cit*., nota 117, p. 1043.

corporal sobre el que la acción típicamente se realiza[441]. Sin embargo, en la medida en que las conductas no necesariamente recaen sobre objetos corporales en la era de la información y de Internet, parece más acorde con las nuevas tecnologías y con el delito de *hacking* referirnos al objeto material siguiendo a ANTOLISEI[442] como la persona o la cosa sobre la cual recae la actividad física del reo. En el mismo sentido se ha referido también ANTÓN ONECA[443] a la persona o cosa sobre la cual recae materialmente la acción, que en el delito que nos ocupa lo constituye actualmente el sistema de información.

### *4.1 El objeto material en la regulación tras la LO 5/2010.*

Con la LO 5/2010 el artículo 197.3 del CP se refería al acceso no autorizado, con vulneración de las medidas de seguridad, a datos o programas informáticos. En concreto, mientras el apartado 1 del precepto se refiere al apoderamiento de "*papeles*, *cartas*, *mensajes de correo electrónico o cualesquiera otros documentos o efectos personales*" y el apartado 2 al apoderamiento, utilización o modificación de "*datos reservados de carácter personal o familiar de*

441 MEZGER, E., *Tratado de Derecho penal …*, cit., nota 341, p. 316.

442 ANTOLISEI, F., *Manual de Derecho Penal. Parte General*, ed. Temis, Bogotá, 1988, traducida por GUERRERO, J., y AYERRA REDÍN, M., p. 130.

443 ANTÓN ONECA, J., *Derecho Penal*, ed. Akal, segunda edición, anotada y corregida por HERNÁNDEZ GUIJARRO, J.J. y BENEYTEZ MERINO, L., Madrid, 1986, p. 180.

*otro que se hallen registrados en ficheros o soportes informáticos*", el apartado 3 tipificaba el acceso a cualesquiera "*datos o programas informáticos*", por lo que variaba el objeto material.

Por tanto, el objeto del 197.3 del CP lo constituía cualquier dato o programa informático, siendo el objeto material de la acción esos datos o programas informáticos contenidos en un sistema informático o en parte del mismo. En consecuencia, en el supuesto del acceso no autorizado, debía ser un acceso a datos o programas informáticos contenidos en el sistema informático.

Ante la falta de conceptos en el Código Penal, había que acudir a la definición de los datos informáticos que se encontraba en el artículo 1.b) de la DM 2005/222/JAI. En ésta se conceptúa como:

*"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"*[444].

Por tanto, eran unidades básicas de información no legibles por las personas de forma directa.

Respecto a los programas informáticos, había que acudir a la definición que el legislador establecía en el artículo 96.1 de la LPI, es

[444] En el mismo sentido, los datos informáticos se definen en el artículo 2.b) de la Directiva 2013/40/UE como "*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*".

decir:

"*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*".

### *4.2 El objeto material en la regulación tras la LO 1/2015.*

Con la reforma de la LO 1/2015, el legislador modifica el objeto material del delito, pasando de los "*datos o programas informáticos contenidos en un sistema informático o en parte del mismo*" a la referencia "*al conjunto o una parte de un sistema de información*", lo que, como veremos a continuación, supone un adelantamiento de la barrera de protección del bien jurídico y, como señala COLÁS TURÉGANO[445], la acentuación de la tutela de la seguridad y el alejamiento del amparo al otro bien jurídico, la intimidad. Y ello porque no se exige el acceso a los datos o programas informáticos sino que es suficiente con el acceso a todo o parte del sistema de información.

Efectivamente, mientras el artículo 197.1 se refiere al apoderamiento de "*papeles, cartas, mensajes de correo electrónico o cualesquiera otros documentos o efectos personales*", el artículo 197.2

[445] COLÁS TURÉGANO, A., "Nuevas conductas delictivas ...", *cit*., nota 168, p. 677.

al apoderamiento, utilización o modificación de "*datos reservados de carácter personal o familiar de otro que se hallen registrados en ficheros o soportes informáticos*", y el anterior artículo 197.3 introducido por la LO 5/2010 se refería al acceso a cualesquiera "*datos o programas informáticos*", la LO 1/2015 ha introducido el nuevo artículo 197 *bis* 1, que se refiere ahora al acceso "*al conjunto o una parte de un sistema de información*". Esta modificación se produce en atención a lo dispuesto en concordancia con el artículo 2.1 de la DM 2005/222/JAI que establece:

"*Cada Estado miembro adoptará las medidas necesarias para que el acceso intencionado sin autorización al conjunto o a una parte de un sistema de información sea sancionable como infracción penal, al menos en los casos que no sean de menor gravedad*".

Y también resulta de lo establecido en el artículo 3 de la Directiva 2013/40/UE, que dispone:

"*Los Estados miembros adoptarán las medidas necesarias para que, cuando haya sido realizado intencionalmente, el acceso sin autorización al conjunto o a una parte de un sistema de información sea sancionable como infracción penal cuando se haya cometido con violación de una medida de seguridad, al menos en los casos que no sean de menor gravedad*".

De esta forma, como señala CASTELLÓ NICÁS[446], la nueva

[446] CASTELLÓ NICÁS, N., "Delitos contra la intimidad …", *cit*., nota 396, p. 507.

dicción "*sistema de información*" es más amplia que la anterior relativa a "*datos o programas informáticos*", ya que la referencia abarca el propio sistema de información que los contiene. Con ello, se evitan eventuales problemas derivados de un mero acceso al sistema de información, que puede no conllevar un acceso a datos o programas informáticos, pero que puede ser igualmente lesivo para la integridad del sistema. Esto ocurre en el caso citado por SALVADORI[447] al referirse al *cracker* que accedía a un sistema de información e introducía un programa espía con el que podía controlar remotamente el sistema, crear *botnets*[448], enviar *spam*[449], o cualquier otra amenaza para la integridad o disponibilidad del sistema informático que, con la

---

447 SALVADORI, I., "Los nuevos delitos ...", *cit*., nota 106, p. 248.

448 El *botnet* se entiende comúnmente como "*nombre genérico que denomina a cualquier grupo de PC infectados y controlados por un atacante de forma remota. Generalmente, un hacker o un grupo de ellos crea un botnet usando un malware que infecta a una gran cantidad de máquinas. Los ordenadores son parte del botnet, llamados "bots" o "zombies"*. Definición generalmente aceptada y disponible en https://blog.kaspersky.es/que-es-un-botnet/755/, consultado el 9 de octubre de 2016.

449 Podemos entender como spam siguiendo a MIRÓ LLINARES como "*e-mail no solicitado que suele enviarse a un numeroso número de direcciones electrónicas bien a través de una dirección electrónica de las ofrecidas por los servicios de correo gratuitos estilo Hotmail, o bien desde un sistema informático infectado, convertido en botnet y utilizado por el spammer que adquiere las direcciones de correo hackeando sistemas informáticos o utilizando spyware u otros sistemas de búsqueda de direcciones electrónicas a través de la Red*". En MIRÓ LLINARES, F., *El cibercrimen ...*, *cit*., nota 8, p. 308. O, siguiendo a ORTS BERENGUER y ROIG TORRES, simplemente, "*envío masivo de propaganda publicitaria no solicitada a través del correo electrónico. También conocido como junk mail*". En ORTS BERENGUER E. y ROIG TORRES, M., *Delitos informáticos y delitos comunes ...*, *cit*., nota 112, p. 182.

anterior redacción del artículo 197.3 no podía ser castigada.

En una primera aproximación podemos entender pues, con ANARTE BORRALLO y DOVAL PAIS, que por sistema de información hay que entender el "*conjunto de elementos generadores de información mediante el tratamiento y la administración de datos*"[450].

Por tanto, en principio el concepto de sistema de información no tiene porqué ser un sistema informático. Y ello porque aquél es definido en el artículo 5.2.m) de Reglamento de desarrollo de la LOPD como "*conjunto de ficheros, tratamientos, programas, soportes y en su caso, equipos empleados para el tratamiento de datos de carácter personal*" y una de las definiciones más extendidas de "*sistema de información*" se encuentra en *Wikipedia* como "*Un sistema de información es un conjunto de elementos orientados al tratamiento y administración de datos e información, organizados y listos para su uso posterior, generados para cubrir una necesidad o un objetivo*"[451].

Sin embargo, la Directiva 2013/40/UE, en la que se inspira la reforma llevada a cabo por la LO 1/2015, está claramente orientada a la tutela de la seguridad de los sistemas informáticos, por cuanto define el sistema de información en su artículo 2.a) como:

---

[450] ANARTE BORRALLO, E. y DOVAL PAIS, A., "Delitos contra la intimidad …", *cit*., nota 380, p. 518.

[451] La definición de *Wikipedia* está disponible en https://es.wikipedia.org/wiki/Sistema_de_informaci%C3%B3n, consultado el 9 de octubre de 2016.

"*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 dicho aparato o grupo de aparatos para su funcionamiento, utilización, protección y mantenimiento*".

En consecuencia, el concepto de sistema de información en la Directiva 2013/40/UE es el mismo que el del artículo 1.a) de la DM 2005/222/JAI[452] que inspiraba la reforma de la LO 5/2010, pero sustituyendo ahora el término que se empleaba en la DM 2005/222/JAI ("*por estos últimos*") por la referencia a "*por dicho aparato o grupo de aparatos*".

Así pues, el legislador no ha introducido en el Código la definición de sistema de información contenida en los instrumentos internacionales, como sí ha ocurrido en otros países como Chipre[453], Portugal[454], Bulgaria[455], Austria[456] o Rumanía[457] en referencia al "sistema informático", razón por la cual el término ha de

---

[452] DM 2005/222, artículo 1.a), define el sistema de información en los siguientes términos: "*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 o mantenimiento*".

[453] *Vid*., *supra* Capítulo II, subepígrafe 2.1.

[454] *Vid*., *supra* Capítulo II, subepígrafe 2.2.

[455] *Vid*., *supra* Capítulo II, subepígrafe 3.2.

[456] *Vid*., *supra* Capítulo II, subepígrafe 4.2.

[457] *Vid*., *supra* Capítulo II, subepígrafe 4.18.

implementarse con la citada normativa comunitaria, donde su definición es similar a la que recogía el artículo 1 del Convenio Europeo sobre Cibercriminalidad para el "sistema informático", definiéndolo como:

"*todo dispositivo aislado o conjunto de dispositivos interconectados o relacionados entre sí, cuya función, o la de alguno de sus elementos, sea el tratamiento automatizado de datos en ejecución de un programa*".

De todo ello se infiere que la interpretación del término más acertada parece la relativa a los "sistemas de información informáticos"[458], dando cobertura también a los accesos a plataformas de redes sociales. En este sentido, señala ALONSO GARCÍA que darse de alta como usuario en alguna de ellas implica la creación de datos de cada usuario que quedan archivados en esa plataforma, siendo la plataforma un ámbito donde también se puede cometer el delito[459].

Por tanto, con la nueva terminología, el legislador evita la anterior referencia del artículo 197.3 a los "*datos o programas informáticos contenidos en un sistema informático o en parte del mismo*". Esa mención a los datos informáticos podía generar problemas para delimitar estas conductas de las previstas en el artículo

458 ANARTE BORRALLO, E. y DOVAL PAIS, A., "Delitos contra la intimidad …", *cit*., nota 380, p. 519.

459 ALONSO GARCÍA, J., *Derecho penal y redes sociales*, ed. Thomson Reuters Aranzadi, primera edición, Navarra, 2015.

197.2, donde también se regula el apoderamiento de "*datos reservados de carácter personal o familiar de otro que se hallen registrados en ficheros o soportes informáticos*" y que, como señalaba TOMÁS-VALIENTE LANUZA[460], podía estar precedido de un acceso no autorizado en el sistema que los alojaba, planteando problemas de delimitación entre unos y otras, tal y como se expondrá en el siguiente Capítulo con ocasión de la conducta. La actual regulación supone una superación de esos problemas interpretativos y una anticipación de las barreras de protección de los bienes jurídicos al recaer la acción sobre todo o parte del sistema de información sin necesidad de alcanzar los datos o programas informáticos.

Por último, la acción podrá recaer sobre todo o una parte del sistema de información, dando así cumplimiento a la previsión contenida en el Convenio Europeo sobre Cibercriminalidad, que refería el acceso ilícito en su artículo 2 a "*todo o parte de un sistema informático*", el artículo 2.1 de la DM 2005/222 relativa al acceso "*al conjunto o una parte de un sistema de información*" y el artículo 3 de la Directiva 2013/40/UE que también se refiere "*al conjunto o una parte*", acentuando de esta forma la tutela de la seguridad de los sistemas de información frente a la mayor protección de la intimidad que suponía la anterior referencia a los datos o programas informáticos, separación y distinción que también resulta del citado

460 TOMÁS-VALIENTE LANUZA, C., "Título X. Delitos contra la Intimidad ...", *cit*., nota 127, p. 803.

Preámbulo XIII de la LO 1/2015[461]. No es necesario por tanto el acceso a datos o programas ubicados en el sistema de información, sino que basta el simple acceso al sistema.

Aunque la referencia a todo o parte del sistema de información pudiera considerarse innecesaria al entender que accedido a una parte se produce la vulneración del todo, considero lógico pensar con HURTADO ADRIÁN que la razón de ser de la distinción se encontraría en los sistemas informáticos conectados a una red de comunicaciones compartida donde, integrados en ella, aunque se pueda declarar la autonomía de cada ordenador, también es cierto que serán parte del "sistema informático distribuido", no resultando superflua la mención a parte de un sistema informático en el tipo[462].

### *5. NATURALEZA JURÍDICA DEL DELITO DE HACKING.*

De los anteriores epígrafes resta por analizar la naturaleza jurídica del intrusismo informático en nuestro ordenamiento jurídico, atendidas las peculiaridades que muestra su bien jurídico protegido y su objeto material.

En principio, podría entenderse que se trata de un delito de medios indeterminados (*por cualquier medio o procedimiento*), sin

461 Respecto al apartado XIII del Preámbulo de la LO 1/2015, *vid*., *supra* subepígrafe 3.1 de este Capítulo.

462 HURTADO ADRIÁN, A., "Accesos informáticos ilícitos ...", *cit*., nota 145, p. 129.

embargo, esta concepción debe matizarse puesto que tanto el anterior artículo 197.3 como el vigente artículo 197 *bis* 1 exigen para el acceso que se produzca la vulneración de medidas de seguridad[463], medio incorporado desde el primer momento en los trámites parlamentarios de la LO 5/2010, incluyendo la previsión del artículo 2.2 de la Decisión Marco 2005/222, que establece:

"*1. Cada Estado miembro adoptará las medidas necesarias para que el acceso intencionado sin autorización al conjunto o a una parte de un sistema de información sea sancionable como infracción penal, al menos en los casos que no sean de menor gravedad.*

*2. Cada Estado miembro podrá decidir que las conductas mencionadas en el apartado 1 sean objeto de acciones judiciales únicamente cuando la infracción se cometa transgrediendo medidas de seguridad".*

Y también incorporando lo establecido en el artículo 2 del Convenio sobre la Ciberdelincuencia:

*"Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno el acceso deliberado e ilegítimo a la totalidad o a una parte de un sistema informático. Cualquier Parte podrá exigir que el delito se cometa infringiendo medidas de seguridad, con la intención de obtener datos informáticos o con otra intención delictiva, o en*

[463] En este sentido, TOMÁS-VALIENTE LANUZA, C., "Título X. Delitos contra la Intimidad ...", *cit*., nota 127, p. 803.

*relación con un sistema informático que esté conectado a otro sistema informático".*

En este último se dejaba libertad a los Estados para incluir esta exigencia en la tipificación de estas conductas. No obstante, siguiendo el texto del artículo 3 de la Directiva 2013/40/UE que establece la necesaria violación de una medida de seguridad, la previsión de este medio en el vigente artículo 197 *bis* 1 está plenamente justificada. En consecuencia, entiendo que se trata de un delito que exige ese medio o procedimiento para el acceso al sitema.

Lo expuesto no resulta aplicable al caso de las conductas de mantenimiento, donde el acceso se deberá haber producido necesariamente sin quebrantar las medidas de seguridad, ya que en caso contrario se estaría ante la anterior conducta, es decir, un acceso ilícito. Así, en el caso de los supuestos de permanencia en el sistema, resultarán indiferentes los medios por los cuales el sujeto cometa el delito, siempre y cuando ese mantenimiento venga precedido de una entrada autorizada al sistema.

Por otra parte, cabe plantearse si el delito de *hacking* es un delito de mera actividad o de resultado.

Sin ánimo de plantear aquí las distintas teorías en torno a una y otra categoría de delitos, siguiendo a QUINTERO OLIVARES el resultado puede consistir en una lesión para el bien jurídico producida por el ataque material a aquello que lo encarna o en la puesta en peligro de bienes jurídicos. Además, se puede entender que los delitos

de resultado se refieren a bienes jurídicos tangibles, que pueden ser menoscabados o destruidos, o puestos en peligro, razón por la cual los tipos penales que se refieren a estos bienes comprenden la acción lesiva y el resultado de destrucción, vulneración, menoscabo o puesta en peligro. Por el contrario, otros bienes jurídicos no pueden ser vulnerados físicamente, sino que se ofenderían por la simple conducta del autor, conducta orientada a una meta. En estos casos, los tipos describen una pura acción, pero que es suficiente para lesionar el bien jurídico protegido[464]. Según exponen ORTS BERENGUER y GONZÁLEZ CUSSAC, las características de los delitos de mera actividad se encuentran en que el tipo se satisface con la sola realización de la acción típica, mientras que en los de resultado se requiere, además, la causación de un resultado, entendiendo como tal "*la causación de una consecuencia distinta de la acción, de la manifestacion de voluntad, por tanto, de la que aparece temporal y espacialmente separada*", sin confundir el resultado con la lesión del bien jurídico protegido[465]. En este mismo sentido, DE VICENTE MARTÍNEZ define como delito de mera actividad aquel cuya descripción y contenido material se agota en la realización de una conducta, sin necesitar que se produzca un resultado separado espacio-temporalmente de ésta, mientras que el delito de resultado requiere que la acción vaya segudia de la causación de un resultado separable

[464] QUINTERO OLIVARES, G., con la colaboración de MORALES PRATS, F., *Parte general del Derecho penal*, ed. Aranzadi, Navarra, 2010, p. 334 y 348.

[465] ORTS BERENGUER, E. y GONZÁLEZ CUSSAC, J. L., *Compendio de Derecho penal, parte general*, ed. Tirant Lo Blanch, Valencia, 2016, p. 244.

espacio-temporalmente de la conducta[466].

En consecuencia, siguiendo a LAURENZO COPELLO, podemos decir que cuando sea posible identificar adecuadamente el objeto de tutela de un determinado delito, si para su consumación se exige la lesión o puesta en peligro concreto de dicho bien, se dan las bases necesarias para afirmar la existencia de un resultado típico, entendido como efecto separable de la acción[467].

Con estos planteamientos, en el caso del acceso al sistema o el mantenimiento no autorizado, entiendo, tal y como se viene anticipando, que no es suficiente con llevar a cabo esa acción típica, sino que se debe ver afectada la seguridad del sistema, razón por la cual nos encontraríamos ante un delito de resultado en ambos supuestos.

Ahora bien, tal y como señala LAURENZO COPELLO, en la categoría de delitos de resultado cabe pensar en la alternativa delitos de resultado y de lesión o delitos de resultado y de peligro[468].

Cabe entonces plantearse, conforme a la definición de delitos de lesión y de resultado de RODRÍGUEZ MONTAÑÉS[469], si nos encontramos ante un delito donde el tipo exige como resultado la

---

466 DE VICENTE MARTÍNEZ, R., *Vademécum de Derecho Penal*, 3º edición, ed. Tirant Lo Blanch, Valencia, 2014, libro electrónico sin numeración de páginas.

467 LAURENZO COPELLO, P., *El resultado en Derecho Penal*, ed. Tirant Lo Blanch Alternativa, Valencia, 1992, p. 177.

468 *Ibíd.*, p. 117.

469 RODRÍGUEZ MONTAÑÉS, T., *Delitos de peligro, dolo, e imprudencia*, ed. Universidad Complutense de Madrid, Madrid, 1994, p. 13.

efectiva destrucción o menoscabo de la seguridad del sistema, es decir, en palabras de MÉNDEZ RODRÍGUEZ, un resultado material de lesión a un bien jurídico[470], o si es suficiente con el peligro para el bien jurídico protegido, con la amenaza del mismo, configurándose como delito de lesión, en el primer caso, o como delito de peligro, en el segundo supuesto.

El artículo 197 *bis* 1 nada dice sobre la efectiva destrucción de la integridad del sistema o su menoscabo, situación que por otra parte daría lugar a un delito de daños del artículo 263 del CP, ni tampoco sobre el menoscabo de su confidencialidad o de su disponiblidad, que también podría encuadrarse según el caso a un delito contra la intimidad del artículo 197 del CP o de nuevo como un delito de daños. Es decir, en el delito de *hacking* no se exige la destrucción o menoscabo efectivo de la seguridad del sistema. Por tanto, no parece que nos encontremos ante un delito de lesión en el caso del acceso al sistema ni en el supuesto del mantenimiento.

En realidad más bien se da la circunstancia de que el acceso o el mantenimiento se castigan porque es posible que con esa conducta se lesione la seguridad del sistema, es decir, empleando los términos de ORTS BERENGUER y GONZÁLEZ CUSSAC parece que el legislador ha optado por adelantar la línea de protección con este tipo, aumentado con esta técnica la tutela de los intereses individuales amenazados por nuevas formas de criminalidad y las nuevas

[470] MÉNDEZ RODRÍGUEZ, C., *Los delitos de peligro y sus técnicas de tipificación*, ed. Universidad Complutense de Madrid, Madrid, 1993, p. 132.

tecnologías[471]. Así, como dice QUINTERO OLIVARES, los delitos de peligro son de importancia creciente político-criminalmente, acudiendo cada vez más a ellos el legislador como consecuencia de los avances de la técnica, con los consiguientes riesgos, y la necesidad de proteger bienes jurídicos de especial importancia que requieren una protección anticipada castigando conductas peligrosas para ellos, sin que esto signifique que el intérprete deba despreciar el cumplimiento de los principios esenciales del Derecho penal[472]. En el mismo sentido MÉNDEZ RODRÍGUEZ destaca el adelantamiento de las barreras de protección penal como una de las características de los delitos de peligro[473]. Y, en palabras de MUÑOZ CONDE y GARCÍA ARÁN, el delito de peligro es el que no exige para su consumación la lesión del bien jurídico sino sólo la amenaza para éste, siendo de peligro concreto cuando el resultado típico consiste en la puesta en peligro del bien jurídico y peligro abstracto cuando se describe una conducta que según la experiencia suele ser peligrosa para un bien jurídico aunque en el caso concreto no lo sea[474].

Si consideramos la concepción de peligro expuesta por MORENO ALCÁZAR, dirigida a entender cualquier delito de peligro,

---

471 ORTS BERENGUER, E. y GONZÁLEZ CUSSAC, J. L., *Compendio de Derecho penal...*, *cit*. nota 465, p. 255.

472 QUINTERO OLIVARES, G., con la colaboración de MORALES PRATS, F., *Parte general ...*, cit., nota 464, p. 349.

473 MÉNDEZ RODRÍGUEZ, C., "Delitos de peligro y bienes jurídicos colectivos", en *Nuevo Foro Penal*, nº 44, junio, 1989, pp. 167, 169, 171.

474 MUÑOZ CONDE, F., y GARCÍA ARÁN, M., *Derecho Penal. Parte General ...*, *cit*., nota 338, p. 325.

éste sería el resultado objetivo sobre el que, realizado un juicio de previsibilidad se llegaría a la conclusión de que la posibilidad de lesionar el bien jurídico que se pretende proteger adquiere relevancia típica[475]. En cada caso será necesario comprobar si el acceso o el mantenimiento ha llegado hasta el punto de ocasionar el resultado del peligro para el sistema, por cuanto como señala el citado autor, es la aparición del resultado de peligro el momento donde se debe situar el juzgador, a diferencia de los delitos de lesión, donde el plano en el que el resultado lesivo se encuentra inserto normalmente salta a la vista[476].

Como indica DOVAL PAIS, mientras con el delito de lesión se pretende proteger la indemnidad o integridad de un objeto, en el delito de peligro la seguridad del objeto ante los riesgos provinientes de ciertos medios es el bien jurídico protegido[477]. Así, para el delito de *hacking* nada dice el tipo sobre la efectiva destrucción del sistema, sino que parece más bien que debe existir un riesgo para la confidencialidad, integridad o disponibilidad del sistema. De esta forma, resulta más acertado afirmar que nos encontramos ante un delito de peligro.

Y en este punto se debe diferenciar entre la categoría de peligro concreto o abstracto, es decir, si como señala RODRÍGUEZ

---

475 MORENO ALCÁZAR, M. A., *El concepto penal de incendio desde la teoría del caos (una perspectiva sistemática de los bienes jurídicos colectivos, del peligro y de su causalidad)*, ed. Tirant Lo Blanch, Valencia, 2002, p. 383.

476 *Ibíd*., pp. 385, 525.

477 DOVAL PAIS, A., *Delitos de Fraude Alimentario*, ed. Aranzadi, Navarra, 1996, p. 212.

MONTAÑÉS, el tipo requiere la concreta puesta en peligro del bien jurídico y el peligro concreto es el resultado típico, en cuyo caso nos encontrariamos ante un delito de peligro concreto, o bien se castiga la acción típicamente peligrosa, sin exigir que en el caso concreto se haya puesto efectivamente en peligro el bien jurídico protegido, caso del delito de peligro abstracto[478].

Además, con MÉNDEZ RODRÍGUEZ podemos considerar que los delitos de peligro concreto constituyen una categoría de delitos de resultado, donde es necesario individualizar un auténtico resultado de peligro para un bien jurídico determinado, mientras que el delito de peligro abstracto se ha convertido en un concepto residual, apto para abarcar todo lo que no sea lesión o peligro concreto para un bien jurídico[479], siendo delitos de peligro concreto aquellos en los que el peligro se configura como un elemento del tipo, por lo que es necesario para la consumación demostrar que en la situación concreta hubo un riesgo para los bienes jurídicos determinados, mientras que en los delitos de peligro abstracto el peligro no es un elemento del tipo sino la razón o el motivo de la tipificación[480].

Así, como exponen ORTS BERENGUER y GONZÁLEZ CUSSAC, el peligro concreto se caracterizaría porque la conducta

---

478 RODRÍGUEZ MONTAÑÉS, T., *Delitos de peligro ..., cit*., nota 469, p. 14.

479 MÉNDEZ RODRÍGUEZ, C., *Los delitos de peligro* ...., *cit*., nota 470, pp. 132 y 227.

480 MÉNDEZ RODRÍGUEZ, C., "Delitos de peligro ...", *cit.,* nota 473, pp. 167, 169, 171.

debe comportar una probabilidad de producción efectiva de daño, esto es, que el objeto de tutela se haya encontrado realmente en riesgo en el caso enjuiciado; mientras que en el delito de peligro abstracto la realización de la conducta resulta en sí misma peligrosa y, por tanto, en sí misma ya está desvalorizada, es decir, el castigo es independiente del riesgo producido en el caso individual pues la peligrosidad pertenece a la acción típica[481]. Y, en palabras de MUÑOZ CONDE y GARCÍA ARÁN, el delito de peligro es el que no exige para su consumación la lesión del bien jurídico sino sólo la amenaza para éste, siendo de peligro concreto cuando el resultado típico consiste en la puesta en peligro del bien jurídico y peligro abstracto cuando se describe una conducta que según la experiencia suele ser peligrosa para un bien jurídico aunque en el caso concreto no lo sea[482].

Por tanto, con estos planteamientos parece que nos encontraríamos ante un delito de peligro concreto porque es necesario que se origine un riesgo para la seguridad del sistema, es decir, concurre la concepción expuesta por RODRÍGUEZ MONTAÑÉS de que el bien jurídico es puesto en una situación de crisis, perturbado en su seguridad, dejando su integridad en manos del azar[483]. Como hemos visto, no estamos ante un supuesto donde el tipo exija la

---

481 ORTS BERENGUER, E. y GONZÁLEZ CUSSAC, J. L., *Compendio de Derecho penal...*, *cit*. nota 465, p. 255.

482 MUÑOZ CONDE, F., y GARCÍA ARÁN, M., *Derecho Penal. Parte General ...*, *cit*., nota 338, p. 325.

483 RODRÍGUEZ MONTAÑÉS, T., *Delitos de peligro ..., cit*., nota 469, p. 37.

destrucción o efectivo menoscabo de la seguridad del sistema, sino que como consecuencia del acceso o el efectivo mantenimiento debe ponerse en peligro la confidencialidad, integridad o disponiblidad del sistema informático. Por tanto, aparece claramente delimitado ese peligro, como un peligro concreto para la seguridad del sistema, es decir, está individualizado un auténtico resultado de peligro para un bien jurídico determinado y ese bien se debe haber encontrado realmente en riesgo en el caso enjuiciado.

Con estos planteamientos, conforme se ha expuesto anteriormente[484], nos encontramos ante un delito con el cual se protege la seguridad de los sistemas de información, pero no se exige su efectiva destrucción o menoscabo, sino que se trata de prevenir los actos atentatorios de la confidencialidad, integridad y disponibilidad de los datos y sistemas informáticos, siempre que haya existido un riesgo real para alguno de ellos, razón por la cual como veremos en el siguiente Capítulo, se producirá la consumación con el acceso en el sistema informático o cuando el sujeto se mantuviese en el sistema después de que existiese una voluntad contraria a esa permanencia, manifestada por el titular del derecho de exclusión, si en cualquiera de los dos casos concurre ese peligro concreto para la confidencialidad, integridad o disponibilidad del sistema.

De no ser así, si fuera suficiente con el acceso o el mantenimiento sin poner en peligro concreto ese bien, es decir, si el castigo fuese independiente del riesgo efectivamente producido,

484 *Vid., supra* subepigrafe 3.5 de este Capítulo.

estaríamos más bien ante un delito de peligro abstracto.

Esta es la postura que parecen mantener ANARTE BORRALLO y DOVAL PAÍS cuando manifiestan que el delito de intrusismo informático sería un delito de peligro abstracto si consideramos que se está protegiendo la seguridad de los sistemas de información y se conecta sistemáticamente con la intimidad, por ser la rúbrica del Título donde se ubica y ser ese el bien jurídico de los delitos comprendidos en el artículo que precede al *hacking*. Incluso se puede hablar de un "abstracto delito de peligro" en este caso, atendidas las características de sus elementos típicos, donde se comprende el acceso, la facilitación del mismo a un tercero y el mantenimiento en el sistema, ofreciendo dudas sobre su alcance las dos primeras. En la primera conducta, por si se requiere o no conocimiento de la información incorporada en el sistema, inclinándose estos autores por la primera posición y, en cuanto a facilitar el acceso, se plantean también las dificultades de las conductas omisivas, porque el texto del artículo nada dice, y la delimitación con el artículo 197 *ter*[485]. A la conducta típica se dedica el epígrafe 2 del siguiente Capítulo.

También se inclina por considerar que estamos ante la categría de peligro abstracto COLÁS TURÉGANO, quien después de destacar la referencia del apartado XIII del Preámbulo de la LO 1/2015 hacia la tutela de la seguridad de los sistemas informáticos, menciona su

[485] ANARTE BORRALLO, E. y DOVAL PAIS, A., "Delitos contra la intimidad …", *cit*., nota 380, p. 517.

configuración como delito de peligro abstracto para la seguridad de las redes informáticas, que podría suponer un riesgo para la intimidad y, en consecuencia, un adelantamiento de la barrera de protección del bien jurídico, ya que la conducta se refiere al sistema informático sin necesidad de acceder o mantenerse en los datos o programas[486].

Sin embargo, entiendo que si el delito de *hacking* se configurase como un delito de peligro abstracto, además de que se estaría contraviniendo la normativa comunitaria que fundamenta la reforma penal en esta materia donde se cita la necesaria prevención de los actos atentatorios de la confidencialidad, integridad y disponbilidad de los sistemas informáticos[487], el delito gozaría de una amplitud que, además de dudosa compatibilidad con los principios de intervención mínima, legalidad y de ofensividad, supondría castigar cualquier conducta de acceso quebrantando medidas de seguridad o mantenimiento no autorizado en un sistema, aunque se tratase de un acceso o un mantenimiento que no haya supuesto un riesgo concreto para la confidencialidad, integridad o disponibilidad del sistema. No parece que cualquier acceso o mantenimiento no autorizado, por el hecho de producirse, deba ser castigado si no ha existido al menos el riesgo efectivo para la seguridad del sistema.

Pensemos en el caso de que un sujeto ha accedido al sistema quebrantando medidas de seguridad, pero la confidencialidad,

---

[486] COLÁS TURÉGANO, A., "Nuevas conductas delictivas ...", *cit*., nota 168, pp. 673 y 677.

[487] *Vid*., nota 409.

integridad o disponibilidad del sistema han quedado intactas, porque el sujeto haya sido inmediatamente expulsado del sistema al existir algún otro tipo de medida que reacciona expulsando a cualquier intruso antes de permitir realizar cualquier operación dentro del sistema. O cualquier supuesto de *hacking* blanco, donde se vulneren medidas de seguridad establecidas en un sistema sin estar autorizado, por ejemplo para ayudar a mejorar la protección de determinados sistemas informáticos recopilando los fallos en sus medidas de seguridad. Si considerásemos que es un delito de peligro abstracto, cualquiera de estas conductas deberían ser castigadas, por inocuas que al final resultasen para la seguridad del sistema.

Por tanto, parece que para evitar ampliar en exceso la interpretación del tipo, el acceso requeriría un resultado, que es la puesta en peligro concreto para la seguridad del sistema, es decir, para la confidencialidad, integridad y disponibilidad del mismo. Esto me lleva a pensar que el instrusismo informático, tanto en el caso de acceso, como en el supuesto de mantenimiento, requiere de un efectivo resultado que es el consistente en la puesta en peligro concreto del citado bien jurídico protegido, por exigirlo así el principio de ofensividad, entendido siguiendo a QUINTERO OLIVARES como efectiva puesta en peligro del bien[488].

Por todo ello, considero que el delito de *hacking* es un delito de peligro concreto para la seguridad del sistema informático afectado,

[488] QUINTERO OLIVARES, G., con la colaboración de MORALES PRATS, F., *Parte general* ..., cit., nota 464, p. 349.

en la medida en que con el acceso al sistema o el mantenimiento no autorizado se habrá puesto en peligro la seguridad específica del sistema informático al que se accede o se permanece, bien en concreto al que como hemos visto se hace expresa referencia en la normativa comunitaria que fundamenta la introducción del tipo en el Código Penal. Sin embargo, puede entenderse que con ese instrusismo se ocasiona también un riesgo para otros bienes jurídicos, como pueden ser los citados por MORALES PRATS: la intimidad, los secretos de empresa o el patrimonio, siempre que se proyecten sobre los datos o programas ubicados en el sistema de información[489]. Esto supone que con el acceso también nos podemos encontrar ante un eventual riesgo o lesión para esos otros bienes ya que, empleando la terminología de HURTADO ADRIÁN, con el delito de *hacking* se anticipan las barreras de protección en relación con eventuales ataques contra bienes jurídicos individuales[490], y esa barrera se adelanta tras la reforma de 2015, en la medida en que la conducta ya no se refiere al acceso a datos o programas a los que se refería el anterior artículo 197.3 CP tras la reforma de la LO 5/2010, sino al conjunto o una parte de un sistema de información.

Por tanto, coexiste el peligro concreto para la seguridad del sistema afectado junto a la posibilidad de un riesgo o efectiva lesión

[489] MORALES PRATS, F., "Delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio", en QUINTERO OLIVARES (Dir.) y VVAA, *Comentarios a la parte especial del Derecho penal*, ed. Aranzadi, Navarra, 2016, p. 470.

[490] HURTADO ADRIÁN, A., "Accesos informáticos ilícitos ...", *cit*., nota 145, p. 127.

para otros bienes jurídicos como son los citados de intimidad, propiedad, patrimonio o secretos de empresa, que no necesariamente debe concurrir y que, caso de producirse, dará lugar al correspondiente concurso, tal y como veremos en el epígrafe 5 del siguiente Capitulo.

### *6. TOMA DE POSICIÓN.*

Tal y como se ha expuesto, la figura presenta dificultades interpretativas desde el momento mismo en el que se analiza su ubicación sistemática.

En atención a la descripción típica parece razonable pensar que el legislador pretende proteger la seguridad de los sistemas, por ser presupuesto insoslayable para que la informática pueda desempeñar su función en la organización social, siendo necesaria su tutela y adelantando de esta forma la barrera de protección de otros bienes jurídicos. Por ello resulta distorsionada su ubicación en el Título X del CP, entre los delitos contra la intimidad.

Desde mi punto de vista, atendiendo a los motivos por los cuales se introdujo el artículo 197.3 del CP por la LO 5/2010 y después el 197 *bis* 1 del CP por la LO 1/2015, referidos a los compromisos internacionales, la seguridad de los sistemas informáticos (abarcando la confidencialidad, la integridad y la disponibilidad de los sistemas informáticos) constituye el bien jurídico directamente protegido por este precepto, atendida además la menor

pena que conllevan estas conductas en relación con las previstas en los apartados 1 y 2 del artículo 197 CP. Estos son los intereses recogidos en el Preámbulo del Convenio Europeo sobre Cibercriminalidad, en los considerandos 1 y 2 de la DM 2005/222/JAI y en el Considerando 26 de la Directiva 2013/40/UE.

Sin embargo, la Directiva 2013/40/UE también menciona en su Considerando 29 como objeto de protección "*el pleno respeto de dichos derechos y principios y debe aplicarse en consecuencia*". Entre estos derechos, el mismo considerando cita expresamente la "*protección de datos de carácter personal, el derecho a la privacidad, la libertad de expresión e información, el derecho a un juicio equitativo, la presunción de inocencia y los derechos de la defensa*"[491]. Por tanto, entre otros derechos, se trata de proteger también los datos de carácter personal y la privacidad, al menos de forma anticipada e indirecta.

En consecuencia, la legislación europea no excluye la protección de la intimidad con este nuevo delito, que es lo que parece

[491] Según dispone el Considerando 29 de la Directiva, "*La presente Directiva respeta los derechos humanos y las libertades fundamentales y cumple los principios reconocidos, en particular, por la Carta de los Derechos Fundamentales de la Unión Europea y el Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales, incluida la protección de datos de carácter personal, el derecho a la privacidad, la libertad de expresión e información, el derecho a un juicio equitativo, la presunción de inocencia y los derechos de la defensa, así como los principios de legalidad y proporcionalidad de las infracciones penales y las sanciones. En especial, la presente Directiva tiene por objeto garantizar el pleno respeto de dichos derechos y principios y debe aplicarse en consecuencia*".

pretender el legislador español al incluir el tipo entre los delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio, si bien en este caso considero que se trata de un bien jurídico protegido de una forma anticipada e indirecta. Este argumento se ve reforzado con el evidente paralelismo entre estas conductas y el allanamiento de morada[492], lo que ha dado lugar a la configuración como bien jurídico del citado domicilio informático[493], así como con las reservas que establece el sujeto pasivo estableciendo las medidas de seguridad, que nos llevan igualmente a la intimidad como bien jurídico protegido de una forma anticipada e indirecta.

Entiendo como MORALES PRATS[494], que este planteamiento del domicilio informático, en la medida en que el domicilio tradicionalmente ha estado vinculado con la seguridad personal, conduce igualmente y no es incompatible con considerar la seguridad del sistema.

Ahora bien, desde mi punto de vista, esa seguridad del sistema

---

492 El artículo 202.1 del CP castiga "*El particular que, sin habitar en ella, entrare en morada ajena o se mantuviere en la misma contra la voluntad de su morador …*".

493 En este sentido, la SAP de Vizcaya de 23 julio de 2014, *cit*., nota 436, se refiere en su FJ 4º al delito tipificado en el anterior artículo 197.3 del CP como un delito "*denominado de intromisión informática en que lo se protege es la libertad informática o más exactamente el domicilio informático de una persona, no siendo relevante la naturaleza de los datos contenidos en el sistema informático pudiendo ser de naturaleza personal, familiar, económicos o de otra índole que pertenezcan al ámbito privado de dicha persona*".

494 MORALES PRATS, F., "Título X. Delitos contra la intimidad ...", *cit*., nota 369, p. 482.

comprende su confidencialidad, integridad y disponibilidad, como bien jurídico protegido de forma directa en el delito que nos ocupa, bien jurídico que además así resulta de la normativa internacional expuesta. Por ello, no comparto que por su ubicación sistemática el acceso ilícito deba proyectarse sobre conductas que potencialmente puedan afectar a la intimidad, sino más bien deberá referirse a los casos en que esa proyección se produzca sobre la citada confidencialidad, integridad y disponibilidad del sistema, porque si se limitara el delito a la intimidad supondría excluir buena parte de los sistemas informáticos públicos, empresariales o políticos que no están referidos a ese derecho, además de que serían numerosos los problemas que se añadirían en su interpretación. Así, comparto el criterio de JORGE BARREIRO[495] relativo al tratamiento separado de estas conductas respecto a las que tutelan la intimidad en un sentido estricto, y lo apuntado por ANARTE BORRALLO y DOVAL PAIS[496], es decir: la falta de referencia en sus elementos a la intimidad, tal y como veremos en el siguiente Capítulo; si se considera como bien jurídico la seguridad de los sistemas de información, supone un adelantamiento de la intervención penal y la cuestión de la legitimidad de la intervención penal; o la falta de mención en la normativa comunitaria a la intimidad en relación con este delito. De igual forma, se plantearía la incongruencia en su aplicación a los

[495] JORGE BARREIRO, A., "Delitos contra la intimidad ...", *cit*., nota 117, p. 1043.

[496] ANARTE BORRALLO, E. y DOVAL PAIS, A. "Delitos contra la intimidad ...", *cit*., nota 380, pp. 497 y 498, 511-513.

supuestos en los que el acceso o el mantenimiento en realidad afecta a intereses mercantiles, institucionales o políticos.

Por otra parte, el conjunto o parte del sistema de información se presenta como el objeto material del delito de *hacking* en nuestro Código.

El hecho de que con la reforma del 2015 se pase de la referencia a los datos o programas informáticos al conjunto o una parte del sistema evidencia el adelantamiento de la protección para los bienes jurídicos individuales que pudieran verse afectados por el acceso y, a su vez, un distanciamiento de la intimidad como bien jurídico protegido.

La amplitud de la nueva terminología, me parece más acertada que la limitada por el acceso a datos o programas informáticos para la tutela del bien jurídico protegido, por cuanto permite incluir supuestos que son igualmente atentatorios contra la seguridad del sistema, como puedan ser los programas espía que se instalan una vez se ha accedido al mismo. Aunque el legislador no ha introducido en el Código un concepto para sistema de información, cabe entender como tal el referido al sistema informático, atendidas las definiciones que ofrecen los instrumentos internacionales que inspiran la reforma llevada a cabo por la LO 1/2015. Además, la referencia expresa al citado objeto material, abandonando los datos o programas informáticos, deja a un lado el problema de delimitación con las conductas del artículo 197.2 CP, relativo al acceso a datos de carácter personal o familiar registrados en ficheros o soportes informáticos.

En cuanto a la descripción del objeto material, como el conjunto o parte del sistema de información, aunque en principio pudiera considerarse innecesario, atendido que quien accede a parte del sistema ya accedido al todo, resulta coherente pensar como HURTADO ADRIÁN que la razón de ser de la distinción se encontraría en los sistemas informáticos conectados a una red de comunicaciones compartida donde, con autonomía propia, también son parte del "sistema informático distribuido"[497].

Por último, el delito va dirigido a proteger la seguridad de los sistemas de información, comprendiendo la confidencialidad, integridad y disponibilidad. El delito de *hacking* se dirige a tutelarlos frente a su puesta en peligro por quien accede ilícitamente al sistema o el que se mantiene sin autorización dentro de él. Se adelantan así las barreras de protección penal, no sólo para evitar la efectiva destrucción de ese bien jurídico concreto, sino también para amparar otros bienes que, conforme a la experiencia, una vez producido el acceso o mantenimiento y puesta en peligro la seguridad del sistema, pudieran verse afectados, como puede ser la intimidad, la propiedad o el patrimonio.

Considero que estamos ante un delito de peligro concreto para la seguridad del sistema informático afectado, en la medida en que con el acceso ilícito al sistema o el mantenimiento no autorizado se deberá haber puesto en peligro la seguridad específica del sistema

[497] HURTADO ADRIÁN, A., "Accesos informáticos ilícitos ...", *cit*., nota 145, p. 129.

informático al que se accede o se permanece. Ello no obstante, con el acceso o el mantenimiento en el sistema también se puede ocasionar un riesgo para otros bienes jurídicos, coexistiendo el peligro concreto para la seguridad del sistema afectado junto a otros eventuales riesgos para otros bienes jurídicos como son los citados de intimidad, propiedad, patrimonio o secretos de empresa. Por todo ello, el delito de *hacking* se puede entender como un delito de peligro concreto para la seguridad del sistema informático afectado pero, a su vez, puede suponer una lesión o puesta en peligro para bienes jurídicos que pueden verse afectados con el acceso o el mantenimiento en el sistema, dando lugar a una relación concursal.

De este modo, atendidos los planteamientos expuestos en el presente Capítulo, entiendo que en el acceso vulnerando medidas de seguridad o en la permanencia no autorizada en un sistema informático, no basta con llevar a cabo esa acción, sino que se debe ver afectada la seguridad del sistema, es decir, debe existir como resultado un peligro efectivo sobre la confidencialidad, integridad o disponiblidad del sistema, bien al que por otra parte se refiere la normativa comunitaria que fundamenta la introducción del tipo en el Código Penal, razón por la cual nos encontraríamos ante un delito de resultado en ambos supuestos.

El tipo no exige la destrucción o menoscabo en la confidencialidad, integridad o disponibilidad del sistema. En los casos que se produjera este resultado más bien cabe pensar en una relación concursal entre el delito de *hacking* que tendría lugar por haber

causado un peligro concreto a ese bien jurídico y un delito de daños del artículo 263 del CP o un delito contra la intimidad del artículo 197 del CP, por la lesión efectivamente producida.

Considero por tanto que el acceso o el mantenimiento se castigan porque es posible que con esa conducta se lesione la seguridad del sistema, es decir, como se ha expuesto, el legislador ha optado por adelantar la línea de protección con este tipo, aumentado con esta técnica la tutela de los intereses individuales amenazados por la aparición de nuevas formas de criminalidad y por las nuevas tecnologías, adelantamiento que es precisamente una de las características de los delitos de peligro.

De esta forma, en cada caso sería necesario comprobar si el acceso o el mantenimiento ha llegado hasta el punto de ocasionar el resultado del peligro para el sistema. En concreto, para su confidencialidad, integridad o disponibilidad. No parece que se deba castigar el mero acceso o mantenimiento sin exigir que se haya puesto efectivamente en peligro el bien jurídico protegido, que lo convertiría en delito de peligro abstracto.

Por tanto, nos encontraríamos ante un delito de peligro concreto porque es necesario que se origine un riesgo para la seguridad del sistema, que es perturbada. No se trataría de un supuesto donde el tipo exija la destrucción o efectivo menoscabo de la seguridad del sistema, sino que como consecuencia del acceso o el efectivo mantenimiento debe ponerse en peligro la confidencialidad, integridad o disponiblidad del sistema informático. Aparece así

claramente delimitado ese peligro, como un peligro concreto.

De esta forma, se trata de prevenir los actos atentatorios de la confidencialidad, integridad y disponibilidad de los datos y sistemas informáticos, siempre que haya existido un riesgo real para alguno de ellos, razón por la cual como veremos en el siguiente Capítulo, se producirá la consumación con el acceso en el sistema informático o cuando el sujeto se mantuviese en el sistema después de que existiese una voluntad contraria a esa permanencia, manifestada por el titular del derecho de exclusión, si en cualquiera de esos dos casos se ha ocasionado el peligro para el citado bien.

De no ser así, si fuera suficiente con el acceso o el mantenimiento sin poner en peligro concreto ese bien, es decir, si el castigo fuese independiente del riesgo efectivamente producido, estaríamos más bien ante un delito de peligro abstracto.

Desde mi punto de vista, si el delito de *hacking* se configurase como un delito de peligro abstracto, además de que en cierta medida se estaría contraviniendo la normativa comunitaria que fundamenta la reforma penal en esta materia, donde se cita la necesaria prevención de los actos atentatorios de la confidencialidad, integridad y disponibilidad de los sistemas informáticos, el delito gozaría de una amplitud que supondría castigar cualquier conducta de acceso quebrantando medidas de seguridad o mantenimiento no autorizado en un sistema, aunque no haya supuesto un riesgo para la confidencialidad, integridad o disponibilidad del sistema, dando prácticamente cabida a cualquier conducta de acceso vulnerando

medidas de seguridad o de mantenimiento no autorizado en el sistema, con la consiguiente posible vulneración de los principios de intervención mínima, legalidad y ofensividad.

Por tanto, el acceso o el mantenimiento no autorizado requieren un resultado, que es la puesta en peligro concreto para la seguridad del sistema, es decir, para la confidencialidad, integridad y disponibilidad del mismo.

Y todo ello no es óbice para entender que con el adelantamiento de las barreras de protección se estén tutelando también otros bienes jurídicos que una vez se produzca el acceso o el mantenimiento en el sistema pudieran verse afectados. Entiendo que esto no implica necesariamente que el tipo se configure como un delito de peligro abstracto, aunque se pueda entender que anticipada e indirectamente se estén tutelando otros bienes jurídicos con el establecimiento de esa barrera anticipada, que pueden ser tan dispares como la intimidad, el patrimonio o la propiedad, cuya efectiva lesión o puesta en peligro más bien dará lugar a la correspondiente relación concursal.

En definitiva, con la reforma llevada a cabo por la LO 1/2015 parece que el legislador no ha sido suficientemente tajante, desaprovechando la ocasión para fijar una clara separación entre los delitos contra la intimidad y el *hacking*, incluso para establecer una regulación unitaria de los delitos informáticos, por cuanto ha optado por dejar el contenido del anterior artículo 197.3 en el siguiente artículo, el 197 *bis* 1, dentro del mismo Capítulo, justificando esta

reforma el que estas conductas, aunque puedan afectar a la privacidad, no están referidas directamente a la intimidad (apartado XIII del Preámbulo). No obstante, esa nueva regulación puede ser un primer paso para una futura agrupación de estos delitos en un apartado propio del Código Penal, de tal forma que se dote de coherencia sistemática al nuevo precepto en relación con el bien jurídico protegido, facilitando su interpretación tal y como ha sucedido en otros países de nuestro entorno como Bélgica, Bulgaria, Croacia, Finlandia o Hungría[498], donde se les ha dedicado un título o capítulo propio y diferenciado.

[498] *Vid*., *supra* Capítulo II, epígrafe 3.

PROGRAMA DE DOCTORADO

"Estudios Jurídicos, Ciencia Política y Criminología"

# EL DELITO DE *HACKING*

TOMO II

TESIS DOCTORAL

Autor: Francisco Almenar Pineda

Directora: Dra. Paz Lloria García

Departamento de Derecho penal

Facultad de Derecho de la Universidad de Valencia

Valencia, mayo de 2017

**ÍNDICE GENERAL**

**TOMO I**

ABREVIATURAS ..... 17

INTRODUCCIÓN ..... 21

CAPÍTULO I. ANTECEDENTES Y EVOLUCIÓN DEL *HACKING* ..... 31

1. INTRODUCCIÓN ..... 33
   - 1.1 El nacimiento de la red y su vinculación con la intimidad..... 33
   - 1.2 El concepto de Derecho penal informático ..... 40
   - 1.3 Rasgos de la delincuencia informática ..... 49
2. EVOLUCIÓN HISTÓRICA ..... 53
   - 2.1 Las primeras manifestaciones ..... 53
   - 2.2 La expansión del uso de Internet ..... 64
   - 2.3 Evolución normativa en el ámbito supranacional ..... 68
3. CONCEPTO DE *HACKING* ..... 80
   - 3.1 El concepto sociológico y gramatical ..... 80
   - 3.2 El concepto normativo ..... 85
4. EL *HACKING* EN EL ORDENAMIENTO PENAL ESPAÑOL ..... 90
   - 4.1 La situación antes de la reforma de 2010 ..... 90
   - 4.2 La justificación de las reformas de los años 2010 y 2015 ..... 105
     - 4.2.1 La reforma del año 2010 ..... 105

4.2.1.1 El Convenio Europeo sobre Cibercriminalidad ..... 107
4.2.1.2 La DM 2005/222/JAI ..... 111
4.2.2 La reforma del año 2015 y la Directiva 2013/40/UE ..... 114
4.3 La tramitación parlamentaria de las reformas de los años 2010 y 2015 ..... 125
4.3.1 La reforma del año 2010 ..... 125
4.3.2 La reforma del año 2015 ..... 145

CAPÍTULO II. BREVE REFERENCIA AL DELITO DE *HACKING* EN EL DERECHO COMPARADO EUROPEO ..... 159

1. INTRODUCCIÓN ..... 161
2. PAÍSES QUE REGULAN LOS DELITOS INFORMÁTICOS EN NORMAS PENALES ESPECIALES.....163
   2.1 Chipre ..... 163
   2.2 Portugal ..... 167
   2.3 Reino Unido ..... 171
3. PAÍSES QUE REGULAN EL DELITO DE *HACKING* EN UN TÍTULO O CAPÍTULO PROPIO Y DIFERENCIADO ..... 178
   3.1 Bélgica ..... 179

3.2 Bulgaria ..... 184
3.3 Croacia ..... 187
3.4 Finlandia ..... 193
3.5 Hungría ..... 197
4. PAÍSES QUE REGULAN EL DELITO DE *HACKING* JUNTO A OTROS DELITOS ..... 203
4.1 Alemania ..... 203
4.2 Austria ..... 207
4.3 Dinamarca ..... 210
4.4 Eslovaquia ..... 214
4.5 Eslovenia ..... 218
4.6 Estonia ..... 220
4.7 Francia ..... 222
4.8 Grecia ..... 227
4.9 Holanda ..... 229
4.10 Irlanda ..... 232
4.11 Italia ..... 238
4.12 Letonia ..... 242
4.13 Lituania ..... 245
4.14 Luxemburgo ..... 248
4.15 Malta ..... 252
4.16 Polonia ..... 257
4.17 República Checa ..... 259
4.18 Rumania ..... 265
4.19 Suecia ..... 268
5. CONCLUSIONES ..... 270

CAPITULO III. BIEN JURÍDICO PROTEGIDO Y OBJETO MATERIAL EN EL DELITO DE *HACKING* ..... 273

1. INTRODUCCIÓN ..... 275
2. PLANTEAMIENTO ..... 278
3. EL DELITO DE *HACKING* COMO DELITO CONTRA LA INTIMIDAD ..... 284
   - 3.1 Introducción ..... 284
   - 3.2 Aproximación al bien jurídico protegido común de los delitos contra la intimidad ..... 286
     - 3.2.1 Evolución histórica ..... 289
     - 3.2.2 Intimidad, secreto, *habeas data* y propia imagen ..... 302
   - 3.3 El *hacking* como delito contra la intimidad ..... 307
   - 3.4 Críticas a la consideración del delito de *hacking* como un delito contra la intimidad ..... 309
   - 3.5 La seguridad de los sistemas informáticos como bien jurídico protegido ..... 317
4. EL OBJETO MATERIAL ..... 331
   - 4.1 El objeto material en la regulación tras la LO 5/2010 ..... 332
   - 4.2 El objeto material en la regulación tras la LO 1/2015 ..... 334
5. NATURALEZA JURÍDICA DEL DELITO DE *HACKING* ..... 341
6. TOMA DE POSICIÓN ..... 356

**TOMO II**

CAPÍTULO IV. EL DELITO DE *HACKING* ..... 379

1. INTRODUCCIÓN ..... 381
2. EL ARTÍCULO 197 *BIS* 1 CP ..... 388
   - 2.1 Los sujetos ..... 391
     - 2.1.1 Sujeto activo ..... 393
     - 2.1.2 Sujeto pasivo ..... 394
   - 2.2 La conducta típica ..... 396
     - 2.2.1 El verbo típico: "acceder a un sistema de información" ..... 400
     - 2.2.2 La exigencia de "medidas de seguridad establecidas para impedirlo" ..... 410
     - 2.2.3 El concepto de no "estar debidamente autorizado"..... 417
     - 2.2.4 Los elementos delimitadores de facilitar el *hacking* en el artículo 197 *bis* 1 en relación con las conductas del nuevo artículo 197 *ter* ..... 436
     - 2.2.5 Los elementos delimitadores del *hacking* en relación con la conducta de mantenimiento en el sistema de información (artículo 197 *bis* 1) . 445
3. POSICIÓN PERSONAL ..... 453
   - 3.1 Planteamiento ..... 453
   - 3.2 Respecto al elemento de acceder a un sistema de información ..... 459

3.3 Las medidas de seguridad establecidas para impedirlo ..... 461

3.4 No estar debidamente autorizado ..... 462

3.5 Elementos delimitadores de facilitar el *hacking* en el artículo 197 *bis* 1 en relación con las conductas del nuevo artículo 197 *ter* ..... 464

3.6 Elementos delimitadores del *hacking* en relación con la conducta de mantenimiento en el sistema de información ..... 468

4. ASPECTO SUBJETIVO ..... 472

5. FORMAS DE APARICIÓN ..... 476

5.1 Autoría y participación ..... 477

5.1.1 Autoría ..... 480

5.1.2 Participación ..... 485

5.2 *Iter Criminis* ..... 492

5.2.1 Actos preparatorios ..... 494

5.2.2 Tentativa ..... 496

5.2.3 Consumación ..... 507

5.3 Relaciones concursales ..... 509

5.3.1 El *hacking* del artículo 197 *bis* 1 y la conducta del artículo 197 *ter* ..... 510

5.3.2 El *hacking* del artículo 197 *bis* 1 y el allanamiento de morada de los artículos 202.1 y 203.1 ..... 512

5.3.3 El *hacking* del artículo 197 *bis* 1 y las conductas del artículo 197.2 ..... 514

5.3.4 El *hacking* del artículo 197 *bis* 1 y las conductas del artículo 264..... 516

5.3.5 El *hacking* del artículo 197 *bis* 1 y otros delitos ..... 517

6. TOMA DE POSICIÓN ..... 522

6.1 Aspecto subjetivo ..... 522

6.2 Autoría y participación ..... 524

6.3 *Iter criminis* ..... 529

6.4 Relaciones concursales ..... 535

CAPÍTULO V. LOS TIPOS AGRAVADOS DEL *HACKING* ..... 541

1. INTRODUCCIÓN ..... 543
2. EL TIPO AGRAVADO DEL ARTÍCULO 197 *QUATER* . 550

2.1 Fundamento del tipo agravado ..... 550

2.2 La conducta del artículo 197 *quater* ..... 561

2.3 Posición personal ..... 576

3. EL TIPO AGRAVADO DEL ARTÍCULO 198 ..... 583

3.1 El concepto de "autoridad o funcionario público" .. 587
3.2 La actuación "fuera de los casos permitidos por la Ley"..... 593
3.3 La actuación "sin mediar causa legal por delito" ..... 600
3.4 La actuación "prevaliéndose de su cargo" ..... 602
3.5 Punto de vista personal ..... 607

CAPÍTULO VI. RESPONSABILIDAD PENAL DE LAS PERSONAS JURÍDICAS EN EL DELITO DE *HACKING* ..... 617

1. INTRODUCCIÓN ..... 619
2. RESPONSABILIDAD PENAL DE LA PERSONA JURÍDICA EN EL DELITO DE *HACKING* ..... 628
   2.1 Planteamiento ..... 628
   2.2 Aproximación al concepto de persona jurídica en el delito de *hacking* ..... 633
   2.3 Las conductas llevadas a cabo por sus representantes legales o por quienes están sometidos a su autoridad .. 647
   2.4 La exigencia de responsabilidad penal a la persona jurídica por el delito de *hacking* ..... 658
3. TOMA DE POSICIÓN ..... 671

CONCLUSIONES ..... 679

ÍNDICE DE DOCUMENTOS ..... 719

JURISPRUDENCIA CONSULTADA ..... 749

BIBLIOGRAFÍA CONSULTADA ..... 761

# CAPÍTULO IV.

# EL DELITO DE *HACKING*.

*1. INTRODUCCIÓN.*

Las conductas de intrusismo informático o *hacking* no tenían una tipificación específica con anterioridad a la LO 5/2010, lo que no suponía que quedaran impunes. Así, si el *hacking* era el medio para cometer otra infracción, la sanción de ésta comprendería ese acceso al sistema informático (por ejemplo, en el caso de la estafa informática del artículo 248.2 del CP), que incluso podría ser penado como tentativa en esos supuestos, lo que también podría darse en el acceso no autorizado al sistema informático como medio para atentar contra la intimidad en los casos de los apartados 1 ó 2 del artículo 197 del CP, relativos, respectivamente, a las actividades tendentes al descubrimiento de secretos o vulneración de la intimidad y al apoderamiento, utilización o alteración de datos registrados, tal y como venimos exponiendo. De esta forma, en todos esos casos el intrusismo informático era una forma de tentativa de esas conductas tipificadas cuando no llegaba a consumarse el delito o bien quedaba absorbido en esos supuestos cuando sí se producía la consumación, tal y como veremos en el presente Capítulo.

La propuesta de penalizar estas conductas de *hacking* de forma autónoma se incluyó en los textos elaborados en los últimos años para la reforma del Código Penal, y finalmente fue incorporado a su artículo 197.3 con la LO 5/2010, precepto que se ha visto sustituido por el artículo 197 *bis* 1 tras la LO 1/2015 como consecuencia de la LO 2013/40/UE.

Tal y como se viene exponiendo, el derogado apartado 3 del

artículo 197 CP se refería al acceso no autorizado, con vulneración de las medidas de seguridad, a datos o programas informáticos. Aunque fue introducido por la LO 5/2010, en este precepto no había referencia a los ataques o daños contra sistemas de información ajenos, mencionados en el apartado XIV del Preámbulo[499] de la referida Ley Orgánica, que fueron llevados al artículo 264. Tampoco el nuevo artículo 197 *bis* 1, introducido por la LO 1/2015 y que traslada el contenido del anterior artículo 197.3 a ese nuevo precepto, se ocupa de los ataques o daños a sistemas informáticos a pesar de que, como se dice en los apartados I y XIII del Preámbulo, con esta reforma se trata de "*la transposición de la Directiva 2013/40/UE, de 12 de agosto, relativa a los ataques contra los sistemas de información*". Tal y como se expone en sus considerandos, esta Directiva se justifica por la importancia de los sistemas de información en la Unión para la interacción política, social y económica, siendo los ataques a estos sistemas una amenaza creciente en el ámbito comunitario, vuelve a incluir el acceso ilícito y amplía las conductas anteriormente previstas

499 "*En el marco de los denominados delitos informáticos, para cumplimentar la Decisión Marco 2005/222/JAI, de 24 de febrero de 2005, relativa a los ataques contra los sistemas de información, se ha resuelto incardinar las conductas punibles en dos apartados diferentes, al tratarse de bienes jurídicos diversos. El primero, relativo a los daños, donde quedarían incluidas las consistentes en dañar, deteriorar, alterar, suprimir o hacer inaccesibles datos o programas informáticos ajenos, así como obstaculizar o interrumpir el funcionamiento de un sistema informático ajeno. El segundo apartado se refiere al descubrimiento y revelación de secretos, donde estaría comprendido el acceso sin autorización vulnerando las medidas de seguridad a datos o programas informáticos contenidos en un sistema o en parte del mismo*".

en la DM 2005/222 con la incorporación de la interceptación ilegal de transmisiones de datos informáticos.

Sin embargo, en el caso de la LO 1/2015 el legislador ha optado esta vez por explicar en el apartado XIII del Preámbulo la separación entre los daños y las interferencias en los sistemas de información para hacer posible distintas respuestas atendida la gravedad de los hechos. Así, dispone su texto que "*Se regulan separadamente, de un modo que permite ofrecer diferentes niveles de respuesta a la diferente gravedad de los hechos, los supuestos de daños informáticos y las interferencias en los sistemas de información*".

En este sentido, señala LUZÓN CUESTA que en la formulación del tipo se pueden utilizar elementos descriptivos, en los que se representa un comportamiento apreciable por los sentidos, como la muerte de otra persona en el homicidio, o elementos normativos, donde será necesario un juicio de valor por parte del intérprete, pudiendo ser elementos normativos jurídicos, donde el juicio de valor se realiza conforme a normas jurídicas, o normativos culturales o sociales, en el que se lleva a cabo conforme a las pautas culturales[500]. Entre unos y otros se encuentran, según MEZGER, los "elementos cognitivos del juicio", que ha de realizar el Juez, que debe llevar a cabo un juicio con arreglo a la experiencia y a los

[500] LUZÓN CUESTA, J. M., *Compendio de Derecho Penal ..., cit.*, nota 12, p. 57.

conocimientos que proporciona[501].

En el caso del *hacking* estamos ante un tipo que, como veremos en este Capítulo, contiene elementos descriptivos (acceso), normativos jurídicos (sistema de información), normativos culturales o sociales (medidas de seguridad), y cognitivos (no estar debidamente autorizado).

Se trata de un precepto con una estructura que comprende dos conductas típicas distintas, al igual que el anterior artículo 197.3. Una primera conducta, consistente en el acceso ilícito a datos o programas informáticos, prevista desde el inicio en el Proyecto publicado el 15 de enero de 2007[502] y mantenida en el nuevo artículo 197 *bis* 1, aunque éste incluye como novedad respecto al citado 197.3 el facilitar el acceso. La segunda, la de permanencia en el sistema informático, que no estaba prevista en la Decisión Marco 2005/222, ni en el Convenio sobre la Ciberdelincuencia, ni en la Directiva 2013/40/UE que ha motivado la reforma por la LO 1/2015.

---

501 MEZGER, E., *Tratado de Derecho penal* ..., *cit*., nota 341, p. 321.

502 Disponible en http://www.congreso.es/public_oficiales/L8/CONG/BOCG/A/A_119-01.PDF, consultado el 7 de octubre de 2016. En relación con el que sería finalmente el artículo 197.3, el texto establecía: "*En el artículo 197 se introduce un nuevo apartado 3, pasando los actuales apartados 3, 4, 5 y 6 a ser los apartados 4, 5, 6 y 7, y se añade el apartado 8, que quedan redactados como siguen: «3. El que por cualquier medio o procedimiento y vulnerando las medidas de seguridad establecidas para impedirlo, accediera sin autorización a datos o programas informáticos contenidos en un sistema informático o en parte del mismo, será castigado con pena de prisión de seis meses a dos años.»*

Estos supuestos de mantenimiento en sistemas informáticos fueron introducidos en el Anteproyecto aprobado por el Consejo de Ministros el 23 de julio de 2009[503]. El texto del Anteproyecto también incluía la referencia a la responsabilidad de las personas jurídicas y su texto dio paso al Proyecto publicado en el BOCG de 27 de noviembre de 2009[504]. Por tanto, este grupo de comportamientos relativos a la permanencia en el sistema constituye una novedad introducida por la LO 5/2010 en el Código penal, similar a la del artículo 615 *ter* del

---

503 Texto del Anteproyecto disponible en http://www.juecesdemocracia.es/LegislacionActual/CP_Antepro_23_07_09.pdf, consultado el 7 de octubre de 2016. El texto del Anteproyecto finalmente aprobado por el Consejo de Ministros el 23 de julio de 2009 introduce como novedad respecto al texto anterior la referencia al mantenimiento no autorizado en un sistema informático y la responsabilidad de las personas jurídicas por estos delitos: "*En el artículo 197 se introduce un nuevo apartado 3, pasando los actuales apartados 3, 4, 5 y 6 a ser los apartados 4, 5, 6 y 7, y se añade el apartado 8, que quedan redactados como siguen: «3. El que por cualquier medio o procedimiento y vulnerando las medidas de seguridad establecidas para impedirlo, accediera 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.*

*Cuando del delito fuere responsable una persona jurídica de acuerdo con lo establecido en el artículo 31 bis de este Código, se le impondrá la pena de multa del tanto al duplo del perjuicio causado.*

*8. Si los hechos descritos en los apartados anteriores se cometiesen en el seno de una organización o grupo criminales, se aplicarán respectivamente las penas superiores en grado.»".*

504 El texto del Proyecto publicado el 27 de noviembre de 2009 está disponible en http://www.congreso.es/public_oficiales/L9/CONG/BOCG/A/A_052-01.PDF#page=1, consultado el 7 de octubre de 2016.

Código penal italiano[505], con el paralelismo entre el sistema informático donde actúa el individuo en red y el domicilio de las personas como su espacio físico y siendo mantenido también en el nuevo artículo 197 *bis* 1 del CP, tal y como se expone en los siguientes epígrafes.

En principio, como se ha adelantado en el anterior Capítulo, podría entenderse que se trata de un delito de medios indeterminados (*por cualquier medio o procedimiento*). Sin embargo, esta concepción debe matizarse por cuanto tanto el anterior artículo 197.3 como el vigente artículo 197 *bis* 1 exigen para el acceso que se produzca la vulneración de medidas de seguridad[506], medio incorporado desde el primer momento en los trámites parlamentarios de la LO 5/2010, incluyendo la previsión del artículo 2.2[507] de la Decisión Marco 2005/222 y del artículo 2[508] del Convenio sobre la Ciberdelincuencia,

---

505 *Vid*., nota 288.

506 En este sentido, TOMÁS-VALIENTE LANUZA, C., "Título X. Delitos contra la Intimidad ...", *cit*., nota 127, p. 803.

507 Artículo 2 de la DM 2005/222: "*1. Cada Estado miembro adoptará las medidas necesarias para que el acceso intencionado sin autorización al conjunto o a una parte de un sistema de información sea sancionable como infracción penal, al menos en los casos que no sean de menor gravedad. 2. Cada Estado miembro podrá decidir que las conductas mencionadas en el apartado 1 sean objeto de acciones judiciales únicamente cuando la infracción se cometa transgrediendo medidas de seguridad*".

508 El artículo 2 del Convenio sobre la Ciberdelincuencia, *cit*., nota 93, establece: *"Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno el acceso deliberado e ilegítimo a la totalidad o a una parte de un sistema informático. Cualquier Parte podrá exigir que el delito se cometa infringiendo medidas de seguridad, con la intención de obtener datos*

que dejaba a la libertad de los Estados incluir esta exigencia en la tipificación de estas conductas. No obstante, siguiendo el texto del artículo 3 de la Directiva 2013/40/UE que establece la necesaria violación de una medida de seguridad, la previsión de este medio en el vigente artículo 197 *bis* 1 está plenamente justificada.

De la citada estructura resulta que el elemento esencial en la conducta de acceso en el sistema informático radica en que la acción se realice "*sin estar debidamente autorizado*". Esto significa que, como veremos, para la conducta del mantenimiento es preciso un previo acceso lícito, por ejemplo, el informático que permanece en un sistema más tiempo del debido para solucionar una avería. Si existiese un previo acceso ilícito nos encontraríamos ante la primera de las conductas mencionadas.

Por otra parte, constituyen una novedad introducida por la LO 1/2015 en el artículo 197 *ter* las conductas consistentes en producir, adquirir para su uso, importar o facilitar a terceros, con la intención de facilitar la comisión de estos delitos, programas o contraseñas sin autorización, en lo que en principio plantea un problema de delimitación con los supuestos de facilitar el *hacking* contemplados en el artículo 197 *bis* 1, tal y como se expondrá en este Capítulo.

Por último, con la reforma de la LO 1/2015 dejan de aplicarse para los delitos de *hacking* los restantes tipos agravados previstos en el anterior artículo 197. En concreto, ahora se refieren a las conductas

---

*informáticos o con otra intención delictiva, o en relación con un sistema informático que esté conectado a otro sistema informático".*

del nuevo artículo 197 pero no al intrusismo informático, que ha salido de ese precepto al artículo 197 *bis* 1. Así, las agravantes previstas en: (i) el artículo 197.4, consistente en si se difundían, revelaban o cedían a terceros los datos o hechos descubiertos o las imágenes captadas, que pasan al nuevo artículo 197.7; (ii) el artículo 197.5, cuando esas conductas eran realizadas por las personas encargadas o responsables de los ficheros, soportes informáticos, electrónicos o telemáticos, archivos o registros, que se trasladan al nuevo artículo 197.4; (iii) el artículo 197.6, relativo a cuando los hechos afectaban 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, que se incorpora al nuevo artículo 197.5; y (iv) el artículo 197.7, en referencia a hechos realizados con fines lucrativos, que se introduce en el nuevo artículo 197.6.

En consecuencia, considerando la configuración típica del artículo 197 *bis* 1, este apartado del trabajo está dedicado al estudio del tipo básico, para más adelante analizar los tipos agravados de los artículos 197 *quater* y 198 CP.

### *2. EL ARTÍCULO 197 BIS 1 CP.*

Tal y como hemos visto, la conducta básica del delito de *hacking* se encuentra prevista en el artículo 197 *bis* 1 CP, que

establece:

"*El que por cualquier medio o procedimiento, vulnerando las medidas de seguridad establecidas para impedirlo, y sin estar debidamente autorizado, acceda o facilite a otro el acceso al conjunto o una parte de un sistema de información o se mantenga en él 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*".

Por tanto, este precepto se ocupa tanto del acceso ilícito como del mantenimiento o permanencia no autorizada en un sistema informático, lo cual según QUERALT JIMÉNEZ[509] supone la tipificación de un acto preparatorio punible por cuanto la intrusión por intrusión, aunque es posible, al resultar inútil, no es fácil que mueva o despierte muchos ánimos criminales.

En una primera aproximación, en el capítulo primero del presente trabajo se ha hecho referencia al concepto de acceso ilícito o *hacking*, razón por la cual en este punto conviene matizar que el artículo 197 *bis* 1 del CP no se refiere al *hacking* como cualquier acceso a un sistema informático, sino que también requiere de otros requisitos que se van a analizar a continuación: vulnerar las medidas de seguridad establecidas para impedirlo, que se realice con ausencia de autorización y que se acceda al sistema de información o parte del mismo.

---

509 QUERALT JIMÉNEZ, J. J., *Derecho penal español ..., cit.*, nota 11, p. 338.

El segundo grupo de conductas reguladas en el mismo precepto, las relativas a la permanencia o mantenimiento en el sistema informático, según se ha descrito, no son propiamente un acceso ilícito al sistema informático. Tal y como se ha manifestado, no hablamos de *hacking*, en un sentido gramatical, sino del mantenimiento en un sistema informático de quien ha accedido lícitamente, que recibe la consideración normativa de *hacking*.

En este caso, el mantenimiento es el "*efecto de mantener o mantenerse*", es decir, "*proseguir en lo que se está ejecutando*"[510]. Se trata, como hemos visto, de conductas omisivas de parada o permanencia abusiva en el sistema de información[511].

Por tanto, normativamente la definición de mantenerse equivale a su concepto genérico. Pero el mantenimiento al que se refiere el artículo 197 *bis* 1 del CP necesita un previo acceso lícito, por cuanto en caso contrario sería propiamente la primera de las conductas del precepto, además requiere la voluntad en contra de quien tenga el legítimo derecho a excluirlo, si bien en este caso no parece necesaria la existencia de medidas de seguridad en el sistema informático, tal y como veremos al final de este epígrafe.

De todo ello resulta necesario delimitar estos conceptos para intentar averiguar el alcance del delito de *hacking* en el nuevo artículo

---

[510] Definición de la RAE disponible en http://lema.rae.es/drae/?val=acceso, consultado el 14 de septiembre de 2015.

[511] SALVADORI, I., "Los nuevos delitos informáticos ...", *cit*., nota 106, p. 233.

197 *bis* 1 del CP, empezando por los sujetos, pues sólo conociendo las conductas a las que se refiere el precepto podremos plantear cuestiones como en qué consiste facilitar esta conducta, que se va a analizar también en este Capítulo, o la comisión de estos delitos en el seno de una organización o grupo criminal, que veremos en el Capítulo V.

### *2.1 Los sujetos.*

Tanto si consideramos el concepto de acción como si nos referimos a la definición del delito, llegamos a la conclusión, como advierten entre otros ORTS BERENGUER y GONZÁLEZ CUSSAC[512], que al Derecho penal sólo le interesa la conducta humana.

En principio se podría considerar con CARRARA[513] que sujeto activo es el hombre que delinque, mientras los instrumentos de los que se sirve son el sujeto activo secundario, considerándose sujeto pasivo del delito el hombre o la cosa sobre que recaen los actos materiales del culpable, encaminados a un fin malvado. Sin embargo, parece más corriente, tal y como señala ANTÓN ONECA, reservar ese último

---

512 ORTS BERENGUER, E. y GONZÁLEZ CUSSAC, J. L., *Compendio de Derecho ..., cit*., nota 465, p. 305.

513 CARRARA, F., *Programa de Derecho Criminal. Parte general. Volumen I*, ed. Temis, Bogotá, 1988, traducido por ORTEGA TORRES, J. J., y GUERRERO, J., p. 52.

concepto para el objeto material del delito[514], al que se ha dedicado el Capítulo anterior de este trabajo, y entender con ANTOLISEI que sujeto activo es el que comete un ilícito penal mientras que sujeto pasivo es la persona ofendida por el delito, la víctima del delito o, de forma más precisa, "*el titular del interés cuya ofensa constituye la esencia del delito*"[515].

Tal y como señala LUZÓN CUESTA, aunque frecuentemente se utilizan como sinónimos sujeto activo y autor, sin embargo, mientras que sujeto activo es quien realiza el comportamiento típico, el concepto de autor, al que se dedicará parte del presente Capítulo, conlleva implícita la responsabilidad criminal por el hecho[516], dicho en otras palabras y siguiendo a ORTS BERENGUER y GONZÁLEZ CUSSAC, el sujeto activo constituye una parte más del tipo de acción, es decir, el sujeto de la disposición que lo define, integrándose en el campo normativo, no real, al que pertenecería el autor[517].

514 ANTÓN ONECA, J., *Derecho Penal ...*, *cit*., nota 443, p. 180.

515 ANTOLISEI, F., *Manual de Derecho Penal ...*, *cit*., nota 442, pp. 121 y 128.

516 LUZÓN CUESTA, J. M., *Compendio de Derecho Penal ...*, *cit*., nota 12, p. 191.

517 ORTS BERENGUER, E. y GONZÁLEZ CUSSAC, J. L., *Compendio de Derecho penal ...*, *cit*., nota 465, p. 305.

*2.1.1 Sujeto activo.*

En principio, siguiendo a QUERALT JIMÉNEZ[518] y a JORGE BARREIRO[519], podemos decir que sujeto activo del delito de *hacking* puede ser cualquiera, configurándose como un delito común, aunque como señala MIRÓ LLINARES, lo más usual es que quien realice el acceso sea una persona con conocimientos informáticos necesarios para llevar a cabo una conducta que en principio se presenta como tecnológicamente compleja[520].

Por otra parte, como indican ANARTE BORRALLO y DOVAL PAÍS[521], aunque nos encontramos ante un delito común, donde cualquiera puede ser sujeto activo y existen peculiaridades en cuanto al sujeto pasivo, el intrusismo informático también tiene su modalidad especial en el artículo 198 CP, referido a los supuestos en los que el delito es llevado a cabo por autoridad o funcionario público, fuera de los casos permitidos por la ley, sin mediar causa por delito y prevaliéndose de su cargo, a la que se hará referencia en el Capítulo V, configurándose en este caso como un delito especial impropio.

---

518 QUERALT JIMÉNEZ, J. J., *Derecho penal español ...*, *cit*., nota 11, p. 339.

519 JORGE BARREIRO, A., actualizado por GUÉREZ TRICARICO, P. "Delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio", en MOLINA FERNÁNDEZ, F. (Coord.) y VVAA, *Memento práctico penal 2017*, ed. Francis Lefebvre, Madrid, 2016, p. 1066.

520 MIRÓ LLINARES, F., "Los Delitos Informáticos ...", *cit*., nota 108, p. 147.

521 ANARTE BORRALLO, E. y DOVAL PAIS, A., "Límites de la ley penal ...", *cit*., nota 24, p. 16.

De forma más concreta, en la conducta que ahora nos ocupa el sujeto activo será quien acceda a todo o parte del sistema informático con la falta de autorización debida que, como se va a exponer en el subepígrafe 2.2.3, además de provenir del propietario del sistema o del titular legítimo, también podrá proceder de la autoridad judicial que autorice el acceso en los casos legalmente previstos.

*2.1.2 Sujeto pasivo*.

Por su parte, el sujeto pasivo también podrá ser cualquiera, si bien en este caso hay que precisar que deberá ser el titular del conjunto o sistema informático sobre el que se lleva a cabo el acceso o el mantenimiento, es decir, el propietario o titular de otro derecho sobre el sistema o parte del mismo, tal y como resulta de la Directiva 2013/40/UE, cuyo artículo 2.d) establece como definición de acceso "*«sin autorización»: un comportamiento al que se refiere la presente Directiva, incluido el acceso, la interferencia o la interceptación, que no haya sido autorizado por el propietario u otro titular del derecho sobre el sistema o parte del mismo o no permitido por el Derecho nacional".*

Al respecto, anteriormente, con el régimen introducido por la LO 5/2010 en el artículo 197.3 CP, ANARTE BORRALLO y

DOVAL PAÍS[522] planteaban los casos en los que el titular del sistema no coincidía con la persona cuyos datos o intimidad pudieran verse afectados por el acceso, concluyendo con que si la persona que accede es la titular del derecho de intimidad o datos afectados, quedaría impune siempre que el sistema no contuviese datos de terceros, mientras que si es un tercero el que accede al sistema que tiene un titular y unos datos pertenecientes a otra persona, cometería un solo delito relacionado tan sólo con el titular de los datos y no del sistema.

No obstante, conviene recordar que el anterior artículo 197.3 CP, en su redacción de la LO 5/2010, hacía referencia al acceso ilícito a datos o programas informáticos, pero atendido el tenor literal de la Directiva 2013/40/UE expuesto, parece que con la reforma de la LO 1/2015 y el planteamiento de la seguridad e integridad del sistema como bien jurídico directamente protegido, se tratará de preservar este bien, con independencia de que el sistema contenga datos de un tercero o del titular del sistema, en cuyo caso, si también se accede a esos datos podrá dar lugar en su caso al correspondiente concurso de normas entre el delito del artículo 197 *bis* 1 CP y el del artículo 197.2 CP, quedando absorbido por éste último[523]. Tal y como indica MIRÓ LLINARES[524], en el caso en el que se acceda a un sistema informático que contenga información de un tercero distinto a su titular, el sujeto

---

522 *Ibid*., p. 17.

523 A las cuestiones concursales se dedica el Capítulo IV, subepígrafe 5.3, de este trabajo.

524 MIRÓ LLINARES, F., "Los Delitos Informáticos ...", *cit*., nota 108, p. 147.

pasivo del delito previsto en el artículo 197 *bis* 1 CP seguirá siendo el titular del sistema, pudiendo existir otro bien jurídico afectado si se accediera a la información con el ánimo de descubrir un secreto.

### *2.2 La conducta típica.*

Según se viene exponiendo, son muy variadas las conductas típicas que tienen cabida en el precepto, comprendiendo los supuestos de empleo de los citados *cracks* o *keygens* en el acceso o, como señala MIRÓ LLINARES[525], es posible el acceso incluso a través de *sniffers* que, siguiendo a este autor, se pueden entender como programas de captura de tramas de información que no están destinadas a él o la persona que rastrea y captura información por la Red por medio de los denominados "*packet sniffers*"[526]. De tal manera que por medio de estos programas sería posible acceder a cada servidor donde se encuentran los correos electrónicos, lo que supone un acceso a todo o parte del sistema de información, que en la mayoría de los casos se llevará a cabo concurriendo los restantes elementos del tipo.

Por otra parte, la referencia a "*o facilite a otro el acceso*" constituye una novedad incluida en el artículo 197 *bis* 1 en el trámite de enmiendas a la que sería finalmente la LO 1/2015. Esta novedad, al igual que el resto del artículo 197 *bis*, fue directamente introducida

525 *Ibíd*., p. 151.

526 MIRÓ LLINARES, F., *El cibercrimen …*, cit., nota 8, p. 308.

con la enmienda 824 propuesta por el Grupo Popular en el Congreso de los Diputados con el siguiente argumentos: "*Las modificaciones propuestas pretenden superar las limitaciones de la regulación vigente para ofrecer respuesta a la delincuencia informática en el sentido de la Directiva 2013/40/UE*"[527].

La conducta de facilitar a otro el acceso no plantea *a priori* problemas desde el punto de vista gramatical, considerando facilitar como "*hacer fácil o posible la ejecución de algo o la consecución de un fin*"[528]. Sin embargo, como indica FRÍAS MARTÍNEZ[529] puede generar problemas de confusión con las conductas del artículo 197 *ter*, donde se establece:

"*Será castigado con una pena de prisión de seis meses a dos años o multa de tres a dieciocho meses el que, sin estar debidamente autorizado, produzca, adquiera para su uso, importe o, de cualquier modo, facilite a terceros, con la intención de facilitar la comisión de alguno de los delitos a que se refieren los apartados 1 y 2 del artículo 197 o el artículo 197 bis: a) un programa informático, concebido o*

[527] Enmienda publicada en el BOCG de 10 de diciembre de 2014 y disponible en http://www.congreso.es/portal/page/portal/Congreso/PopUpCGI?CMD=VERLST&CONF=BRSPUB.cnf&BASE=PU10&PIECE=PUWD&DOCS=1-1&FMT=PUWTXDTU.fmt&OPDEF=Y&QUERY=BOCG-10-A-66-2.CODI, consultado el 8 de octubre de 2016.

[528] Definición de la RAE disponible en http://lema.rae.es/drae/?val=facilitar, consultado el 8 de octubre de 2016.

[529] FRÍAS MARTÍNEZ, E., "Delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio", en ROMA VALDÉS, A. (Dir.) y VVAA. *Código penal comentado*, ed. Bosch, primera edición, Barcelona, 2015, p. 369.

*adaptado principalmente para cometer dichos delitos; o b) una contraseña de ordenador, un código de acceso o datos similares que permitan acceder a la totalidad o a una parte de un sistema de información*".

Por tanto, en este precepto también está previsto facilitar a terceros la comisión del delito del artículo 197 *bis* 1. En principio, y sin perjuicio de un mayor análisis posterior[530], parece que la peculiaridad del artículo 197 *ter* se encuentra en que se refiere a facilitar instrumentos concretos para el acceso (un programa informático, una contraseña de ordenador, un código de acceso o datos similares a una contraseña o un código de acceso), pero precisamente esa ambigüedad en cuanto a facilitar "*datos similares*" a "*una contraseña de ordenador*" o "*un código de acceso*" puede plantear problemas de delimitación en la práctica entre estas conductas y la de facilitar el acceso prevista en el artículo 197 *bis* 1.

La inclusión de estas conductas de facilitar el acceso con la LO 1/2015 supone una tipificación expresa de actos de cooperación elevados a categoría de autoría. De esta forma, como señala COLÁS TURÉGANO[531], en estos casos se produce una criticable ampliación de la autoría a supuestos que con anterioridad a la reforma se habrían considerado como participación. Por ello, para estos casos deberá entenderse que se ha producido un efectivo acceso, por cuanto no

530 *Vid*., subepígrafe 2.2.4 de este Capítulo.

531 COLÁS TURÉGANO, A., "Nuevas conductas delictivas ...", *cit*., nota 168, p. 676.

tendría sentido la citada ampliación del ámbito punible si no se tuviese lugar ese acceso, además de que produciría problemas de delimitación respecto a las conductas del artículo 197 *ter* CP, a las que se hará referencia en el subepígrafe 2.2.4.

A todo ello se añade la posibilidad apuntada por ANARTE BORRALLO y DOVAL PAÍS de incluir las conductas de omisión por quienes tienen el control del acceso y no impiden las intrusiones, ya que el precepto no las excluye[532], y el tipo subjetivo se agotaría en el dolo, que conllevaría el conocimiento y voluntad en cuanto al acceso o permanencia, sobre el conjunto o parte de un sistema de información, sin autorización y que se vulneran las medidas de seguridad establecidas para impedirlo[533].

Por último, no es suficiente con ese acceso, sino que también es preciso que se refiera al "*sistema de información*", la vulneración de "*las medidas de seguridad establecidas para impedirlo*" y no "*estar debidamente autorizado*". Sin estos elementos no existirá el peligro para la seguridad del sistema de información.

Todos ellos constituyen los elementos diferenciales para delimitar el ámbito de protección de la seguridad de los sistemas de información en la conducta de *hacking* del artículo 197 *bis* 1.

---

532 ANARTE BORRALLO, E. y DOVAL PAIS, A., "Delitos contra la intimidad ...", *cit*., nota 373, p. 518.

533 ANARTE BORRALLO, E. y DOVAL PAIS, A., "Límites de la ley penal ...", *cit*., nota 24, p. 13.

### *2.2.1 El verbo típico: "acceder a un sistema de información".*

La importancia del término "*acceda*" radica en que es el verbo típico empleado para calificar la conducta de *hacking* en el artículo 197 *bis* 1. La amplitud que posee su significado permite que tenga cabida todo tipo de acceso, incluyendo el remoto a través de Internet o utilizando la red interna de una empresa. En este sentido, tal y como indica MORALES PRATS, se presenta como un delito de medios indeterminados, que ni siquiera necesita medios comisivos informáticos o remotos en el acceso, comprendiendo así todo tipo de supuestos que hagan posible ese acceso, desde la captación visual contemplando el sistema informático hasta la utilización de una conexión electrónica a través de otro sistema[534].

Así pues, son muy variadas las conductas típicas que tienen cabida en el precepto, incluyendo los supuestos de empleo de los citados *cracks* o *keygens* en el acceso, o como los mencionados *sniffers* o "*packet sniffers*".

En el anterior Capítulo ya hemos visto el concepto de sistema de información como objeto material del delito que nos ocupa y cómo con la nueva terminología introducida por la LO 1/2015, el legislador evita la anterior mención del artículo 197.3 a los "*datos o programas*

[534] MORALES PRATS, F., "Título X. Delitos contra la intimidad …", *cit*., nota 369, p. 484.

*informáticos contenidos en un sistema informático o en parte del mismo*". Esa referencia a los datos informáticos podía generar problemas para delimitar estas conductas de las previstas en el artículo 197.2, donde también se regula el apoderamiento a "*datos reservados de carácter personal o familiar de otro que se hallen registrados en ficheros o soportes informáticos*", que también podía estar precedido de un acceso no autorizado.

En estos casos de acceso, cuando existía vulneración de las medidas de seguridad, requisito exigido por el anterior artículo 197.3, y un acceso a datos de carácter personal o familiar registrados en ficheros o soportes informáticos, conforme al artículo 197.2 anterior y vigente, la solución más acorde con la pena parecía la de ubicar la conducta entre los delitos del artículo 197.2. En otro caso, carecería de sentido premiar al sujeto que accede a esos datos con una pena más benévola (la del anterior artículo 197.3) por el hecho de haber accedido de forma no autorizada y con vulneración de las medidas de seguridad.

Además, otro de los elementos diferenciadores se encuentra en que el *hacking* no exige perjuicio a tercero y, sin embargo, en el caso del acceso previsto en el artículo 197.2, el Tribunal Supremo ha interpretado que es necesario ese elemento. En concreto, la STS de 17 de junio de 2014[535], con cita de otra, en relación con el artículo 197.2,

[535] STS, Sala Segunda, de 17 de junio de 2014, nº 525/2014, nº 525/2014, Pte. Excma. Sra. Dª Ana María Ferrer García (RJ 2014\4513), con cita de otra, FD 6º.

declaraba que:

"*Explica la STS 123/2009, de 3 de febrero que son tres las formas comitivas que se recogen en el mismo: a) el apoderamiento, utilización o modificación de los datos que hemos descrito; b) el mero acceso; y c) la alteración o utilización. El legislador sólo menciona expresamente que la conducta se haga en perjuicio de tercero con relación a la primera y a la tercera de ellas, mientras que no exigiría tal perjuicio en el caso de la conducta de acceso. Sin embargo la STS 990/2012 de 18 de octubre, plantea la necesidad de realizar una interpretación integradora del precepto, en el sentido de que como en el inciso primero se castigan idénticos comportamientos objetivos que en el inciso 2º (apodere, utilice, modifique) no tendría sentido que en el mero acceso no se exija perjuicio alguno, y en conductas que precisan ese previo acceso añadiendo otros comportamientos, se exija ese perjuicio, cuando tales conductas ya serían punibles con la misma pena en el inciso segundo*".

Tampoco la jurisprudencia menor era suficientemente clara en relación con seguir un criterio para aplicar el artículo 197.2 o el anterior artículo 197.3 para castigar el acceso ilícito a redes sociales. Con anterioridad a la reforma de 2010 se ha llegado a considerar atípico el acceso a una cuenta de correo electrónico ajena incluso cuando se ha producido sin consentimiento de su titular, sin cabida en el artículo 197.1 ni en el artículo 197.2 CP, por cuanto, según se decía en la SAP de Madrid, Sección 2ª, de 17 de julio de 2012, los supuestos de apoderamiento de documentos, interceptación de

telecomunicaciones, escuchas y grabaciones de comunicaciones, no pueden ampliarse y aplicarse por analogía al acceso a la cuenta de correo. Según esa misma Sentencia, ese argumento se veía reforzado tras la reforma de la LO 5/2010, donde se incluye expresamente el instrusismo informático, siendo esta la conducta que fue realizada en ese caso, razón por la cual, habiéndose tipificado esa figura específica para el acceso sin autorización, queda constancia de que no podía incluirse en ninguno de los dos apartados anteriores del artículo 197[536].

Sin embargo, una vez aprobada la LO 5/2010 y antes de la reforma de la LO 1/2015, se han dictado resoluciones pronunciándose a favor de incluir el acceso a un correo electrónico dentro de los supuestos del 197.2 por cuanto se entendía que de esta forma se vulneraba la intimidad y se podían conocer datos reservados, existiendo dolo de indiferencia al acceder al correo electrónico. En concreto, el AAP de Barcelona, de 22 de octubre de 2012, en relación con el acceso a la aplicación del correo electrónico ajeno y las diferentes bases de datos contenidas en el sistema, incluso sin llegar a abrir mensaje alguno, puede ser típico por cuanto supone una intromisión en la intimidad que además puede hacer posible el conocimiento de datos reservados. A ello se añade que, según continuaba el citado Auto, el artículo 197.2 *in fine* no requiere de elementos subjetivos de injusto como la intención de descubrir los

[536] SAP de Madrid, Sección 2ª, de 17 de julio de 2012, nº 402/2012, recurso 134/2012, Pte. Ilma. Sra. Dª María del Rosario Esteban Meilan (JUR 2012\282265), FD 2º.

secretos o vulnerar la intimidad de otro, previstos en el artículo 197.1, o el perjuicio de tercero previsto en el principio del artículo 197.2, quizás porque vayan implícitos en la acción. De esta forma:

"*el acusado al acceder a estos archivos, asumió como mínimo con dolo eventual, o por mejor decir de indiferencia, (…) que con su proceder podría vulnerar la legalidad penal, en tanto que el sistema de correo electrónico es un archivo, soporte o fichero que contiene datos, bases de datos e información que pueden ser reservados de carácter personal o familiar de otro"* y por tanto, "*al abrir el sistema de correo electrónico, concurría el elemento subjetivo de volición requerido, en su forma de dolo eventual, siendo suficiente situarse en una posición de indiferencia respecto del contenido posible de la aplicación del correo electrónico, y sin representación, ni posibilidad de acometer ningún acto de averiguación para poder prever el alcance de su conducta*"[537].

No obstante, en sentido contrario también se han dictado otras sentencias:

- La SAP de Valladolid, Sección 4ª, de 18 de marzo de 2011, resolviendo la aplicación del anterior artículo 197.3 en casos de acceso al correo electrónico sin conocimiento ni autorización de su titular, acertando su contraseña de aplicación de correo, manteniendo

[537] AAP de Barcelona, de 22 de octubre de 2012, nº 784/2012, recurso 511/2012, Pte. Ilma. Sra. Dª Elena Guinduláin Oliveras (JUR 2012\372378), FD 2º.

conversaciones con sus contactos haciéndose pasar por él, siendo absuelta "*del delito de revelación de secretos del que venía siendo acusada*", pero, como dice su FD 1º:

"*A nuestro juicio, dicha conducta, si estaría incardinada, al dia de hoy, en el nº 3 del citado art. 197, que no existía al momento de producirse los hechos enjuiciados ("El que por cualquier medio o procedimiento y vulnerando las medidas de seguridad establecidos para impedirlo, acceda si 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..."). Pero es obvio, que dicho precepto no puede ser aplicado en contra del reo* (sic)"[538].

- El supuesto de acceso de la contable de una empresa, desde un equipo informático externo, a los correos corporativos de las trabajadoras, accediendo así al sistema informático de la empresa y al correo de otra trabajadora al obtener por estos medios su nueva contraseña, resuelto por la SAP de Murcia, Sección 3ª,

[538] SAP de Valladolid, Sección 4ª, de 18 de marzo de 2011, nº 102/2011, recurso 52/2011, Pte. Ilmo. Sr. D. José Luis Ruiz Romero (JUR 2011\155178), Antecedente de Hecho Primero y FD 1º.

de 20 de febrero de 2015, donde se exponía en su Antecedente Primero que la acusada:

"*accedió al correo de la trabajadora Dña. Remedios (…), y a través del mismo tuvo conocimiento del correo electrónico de fecha 26/09/11 que el jefe de exportación de TAHE D. Jesús María había enviado al departamento de informática y a los trabajadores de la empresa D. Arturo, D. Enrique, Dña. Amelia y Dña. Remedios, en el que se les comunicaba la finalización de la relación laboral con la empresa de la trabajadora en pruebas Dña. Esmeralda y la nueva contraseña de su correo electrónico ("WILLIAM") para que pudiesen seguir realizando el seguimiento de sus asuntos, y averiguada por la acusada de este modo la nueva contraseña del correo electrónico DIRECCION001, accedió a dicha cuenta (usuario Esmeralda) a las 14:37:50 horas y a las 14:43:48 horas del mismo día 30/09/11 y a las 12:28:18 horas del día 02/10/11, registrando también el visor de sucesos del sistema de seguridad informático de TAHE un acceso a las 12:27:50 del día 02/10/11 a la cuenta de Dña. Adriana (usuario " Adriana "), compañera de la acusada en el departamento de contabilidad de la empresa, y múltiples accesos producidos los días 2, 3 y 4/10/11 nuevamente a la cuenta de Dña. Remedios*

*(usuario " Remedios "), además de los múltiples accesos que se produjeron a la cuenta de ésta última entre las 12:58:37 horas y las 21:15:43 horas del mismo día 30/09/11, accesos todos ellos llevados a cabo desde la dirección de red de origen con el nº I.P. antes mencionado y perteneciente a la acusada*".

Razón por la cual esta Sentencia concluye condenando conforme al artículo 197.3 por cuanto, según su FD 3º se apreciaban los requisitos típicos:

"*acceso inconsentido (la acusada no estaba autorizada en el momento de ejecución de los hechos, lo cual viene a ser reconocido por el propio recurso de apelación); vulneración de las medidas de seguridad informáticas (las mismas existían, se recogen en el relato fáctico y se analizan en el cuerpo de la sentencia, atendiendo a lo expuesto en diversas manifestaciones, entre ellas las de las empleadas de la empresa, su representante legal y el experto informático de la empresa -que incluso es preguntado respecto a las mismas por el Juzgador-); y acceso a correos de empleadas de la empresa, correos corporativos, y a datos y programas informáticos de la empresa*"[539];

[539] SAP de Murcia, Sección 3ª, de 20 de febrero de 2015, nº 88/2015, recurso 184/2014, Pte. Ilmo. Sr. D. Juan del Olmo Gálvez, Antecedente Primero y FD 3º.

- La SAP de Vizcaya de de 23 de julio de 2014, en un supuesto en el que el acusado había realizado tres intentos fallidos de acceso al panel de control de Internet protegido por contraseña y sin autorización de su titular, razón por la cual fue condenado por el delito del anterior artículo 197.3 en grado de tentativa "*al no haber logrado el acusado con la contraseña utilizada acceder al programa informático*"[540].

Con la nueva regulación en el artículo 197 *bis* 1, parece que el legislador ha tratado de solventar el citado problema con la previsión de que el acceso sea al conjunto o una parte de un sistema de información, suprimiendo la anterior previsión del artículo 197.3 relativa al acceso a datos o programas informáticos. Por tanto, no es necesario alcanzar los datos o programas contenidos en el sistema de información, sino que es suficiente con el acceso a todo o parte de él, lo que supone incluir el acceso a la aplicación del correo electrónico ajeno y las diferentes bases de datos contenidas en el sistema, sin necesidad de abrir mensaje alguno.

---

[540] En este sentido, la SAP de Vizcaya de 23 julio de 2014, *cit*., nota 436, FD 4º: "*En este caso y conforme a los hechos declarados probados se ha acreditado la primera modalidad comisiva que conlleva la producción de un resultado cual es el acceso al dato o programa informático y por esa razón al no haber logrado el acusado con la contraseña utilizada acceder al programa informático de Claudio los hechos deben estimarse ejecutados en grado de tentativa*".

Por último, como señala LLORIA GARCÍA, el verbo típico y la flexibilidad o no del bien jurídico determinan la naturaleza permanente o no del delito[541]. Este planteamiento, trasladado al acceso al sistema informático, supone que, no implicando el acceso la afección continuada a la seguridad del sistema informático, entendido como bien jurídico protegido por el delito de *hacking*, da lugar a su configuración como un delito instantáneo en cuanto a las conductas de acceso, es decir, una vez se accede al sistema de información y ha existido un peligro concreto para su confidencialidad, integridad o disponibilidad, la conducta ya ha finalizado, no permaneciendo en el tiempo, faltando la persistencia de uno de los elementos que caracterizan a los delitos permanentes: la continuidad del comportamiento. Supuesto distinto es la permanencia o mantenimiento no autorizado en el sistema, al que se hace referencia en el subepígrafe 2.2.5 de este Capítulo, donde conforme a ese mismo plantamiento estaríamos ante un delito permanente.

En relación con el citado acceso al sistema de información, la vulneración de "*las medidas de seguridad establecidas para impedirlo*" y no "*estar debidamente autorizado*" constituyen los otros dos elementos diferenciales para delimitar el ámbito de protección de su seguridad en la conducta de *hacking* del artículo 197 *bis* 1.

541 LLORIA GARCÍA, P., *Aproximación al estudio del delito permanente*, ed. Comares, Granada, 2006, pp. 61 y 75.

### *2.2.2 La exigencia de "medidas de seguridad establecidas para impedirlo".*

La importancia de las medidas de seguridad en relación con el acceso al sistema de información radica en que si no está protegido, la conducta no será ilícito penal. Además, como indica HURTADO ADRIÁN[542], la situación del sistema protegido evidencia que el titular no quiere que sea accesible. De esta forma, al quebrantarse las medidas de seguridad se incidirá en la falta de autorización que veremos en el siguiente subepígrafe.

Por otra parte, como premisa y como señala COLÁS TURÉGANO, al ser un delito doloso, si el sujeto no tiene la finalidad de quebrantar las medidas de seguridad del sistema, la conducta será atípica, como en el caso del acceso producido por un descuido o negligencia sin la citada intencionalidad[543]. Son conductas que, tal y como dice MORALES PRATS, reclaman insidiosidad, por cuanto al establecerse la medida ya se ha evidenciado la voluntad de que no exista un libre acceso al sistema[544].

Aunque el Convenio Europeo sobre Cibercriminalidad y la DM 2005/222/JAI no imponían el elemento de vulneración de las

---

542 HURTADO ADRIÁN, A., "Accesos informáticos ilícitos ...", *cit*., nota 145, p. 128.

543 COLÁS TURÉGANO, A. "Nuevas conductas delictivas ...", *cit*., nota 168, p. 678.

544 MORALES PRATS, F., "Título X. Delitos contra la intimidad ...", *cit*., nota 369, p. 485.

medidas de seguridad, dejando libertad en este punto a los legisladores nacionales[545], con la reforma de la LO 5/2010 el legislador ha optado por su inclusión en el anterior artículo 197.3 y con la LO 1/2015 se ha mantenido en el artículo 197 *bis* 1, si bien en este caso la Directiva 2013/40/UE que inspira esta reforma exigía expresamente que el acceso "*se haya cometido con violación de una medida de seguridad*" en su artículo 3.

Si atendemos a la definición de la RAE de medida como "*Disposición"* o *"prevención*"[546], desde un punto de vista amplio podríamos entender como medida de seguridad cualquier medio dirigido a garantizar la seguridad del sistema informático, incluyendo tanto los instrumentos o herramientas físicas como las informáticas.

Sin embargo, parece más acorde con las conductas de *hacking* referirnos a las medidas de seguridad conforme al concepto de MIRÓ LLINARES, entendiendo como tales sólo las relativas a la seguridad lógica, en concreto, "*las aplicaciones o herramientas informáticas dirigidas a evitar el hacking o acceso ilícito al sistema y a la información en él contenido*"[547].

---

[545] Así, el artículo 2 del Convenio establece que "*La Partes podrán exigir que el delito se cometa infringiendo medidas de seguridad*" y el artículo 2.2 de la Decisión Marco dispone que "*Cada Estado miembro podrá decidir que las conductas mencionadas en el apartado 1 sean objeto de acciones judiciales únicamente cuando la infracción se cometa transgrediendo medidas de seguridad*".

[546] Definición disponible en http://dle.rae.es/?id=OlAN0dp, consultado el 20 de enero de 2017.

[547] MIRÓ LLINARES, F., "Los Delitos Informáticos ...", *cit*., nota 108, p.

En el mismo sentido se pronuncia FERNÁNDEZ TERUELO considerándolas "*todas aquellas fórmulas que pongan de manifiesto un específico interés por excluir a los demás del acceso al sistema propio y a la información en él contenida*"[548]. Por tanto, quedarían excluidas las medidas que un usuario pueda haber establecido para un fin distinto al acceso, como pudiera ser un mero control de acceso al sistema que no tiene como finalidad impedirlo sino verificarlo. Así se declaraba en la SAP de Alicante de 16 de septiembre de 2015[549], donde se establecía que el acceso empleando una clave que el sujeto tenía por su cargo, no implicaba una vulneración de medidas de seguridad, sino un acceso no autorizado. Así, frente a la postura del Ministerio Fiscal que consideraba que "*dicha vulneración existe por haber utilizado la funcionaria las claves de acceso de que disponía en función de un fin determinado, para obtener información que no le correspondía conocer al estar al margen de sus cometidos en el departamento en que estaba asignada, lo que comporta quebrantar la regularidad de accesos controlada por el sistema informático que exigía una justificación de los mismos en función de los cometidos de cada funcionario*", entiende el Tribunal que:

"*esa circunstancia convierte los accesos en no autorizados, pero no implica la vulneración de medidas de seguridad que exige el*

149.

548 FERNÁNDEZ TERUELO, J. G., *Derecho Penal e Internet …*, *cit.*, nota 82, p. 199.

549 En este sentido, la SAP de Alicante, Sección 10ª, de 16 de septiembre de 2015, nº 351/2015, Pte. Ilmo. Sr. D. Javier Martínez Marfil (JUR 2016\133547), FJ 3º.

*tipo, pues del conjunto de las manifestaciones de los diferentes testigos, lo que se ha denominado "control de acceso" no es más que un registro de los mismos que permite conocer los que se han verificado, por quién y la finalidad con la que se declaran hechos los accesos, pero en modo alguno, consta que incorpore medida específica de seguridad que tienda a excluir el posible acceso de funcionarios concretos, que haya sido necesario burlar por parte de la acusada para obtener las informaciones deseadas*" y "*No puede afirmarse que en este caso se hayan burlado o infringido medidas específicas de seguridad, sino que se ha accedido con contraseñas válidas a informaciones que no se debían conocer, sin que el registro de accesos, más allá de ofrecer una constatación de los mismos, suponga una suerte de barrera que haya que sortear para acceder a los datos, pues carece de características excluyentes para el acceso*".

Además, las medidas de seguridad en principio se limitarían al ámbito interno del sistema, es decir, al *hardware*, entendido como "*conjunto de componentes que integran la parte material*"[550] o "*todos los componentes físicos del sistema informático*"[551], o al *software*, definido como "*conjunto de programas, instrucciones y reglas informáticas para ejecutar ciertas tareas en una computadora*" [552] o "*aplicaciones, datos y programas que hacen funcionar o se ejecutan*

[550] MIRÓ LLINARES, F., *El cibercrimen ...*, *cit*., nota 8, p. 304.

[551] DE LA MATA BARRANCO, N. J. y HERNÁNDEZ DÍAZ, L., "Un ejemplo de delitos informáticos: delitos contra sistemas y datos en el Código penal español, ¿delitos de daños?", en DE LA CUESTA ARZAMENDI, J. L. (Dir.) y VVAA, *Derecho Penal Informático*, ed. Civitas, Pamplona, 2010, p. 201.

[552] MIRÓ LLINARES, F., *El cibercrimen ...*, *cit*., nota 8, p. 308.

*en el sistema informático*"[553].

Esta definición, en clara concordancia con los accesos a sistemas informáticos a los que parece referirse el legislador, nos plantea la duda de si caben otros tipos de medidas de seguridad como puedan ser las de naturaleza física (p.ej. un candado o una llave).

Pues bien, parece evidente que quien establece estas medidas también está tratando de proteger la seguridad o la integridad de su sistema informático intentando evitar su libre acceso, además de que ésta parece ser la fórmula adoptada en otras legislaciones como la rumana, donde el legislador ha incluido expresamente el concepto de medida de seguridad refiriéndolo a cualquier procedimiento, dispositivo o programa dirigido a limitar o prohibir el acceso a un sistema informático a determinados usuarios[554]. De esta forma, la inclusión también de medidas físicas en el concepto de medidas de seguridad resultaría menos problemático referido a cualesquiera aplicaciones o herramientas y no tan sólo a las de naturaleza informática, siempre que hayan sido establecidas específicamente para evitar el *hacking*.

En este sentido, PECORELLA ha planteado si la medida de

---

553 DE LA MATA BARRANCO, N. J. y HERNÁNDEZ DÍAZ, L., "Un ejemplo de delitos informáticos ...", *cit*., nota 551, p. 201.

554 El artículo 35.h) de la LEGE nr. 161 din 19 aprilie 2003, establecía "*h) prin măsuri de securitate se înţelege folosirea unor proceduri, dispozitive sau programe informatice specializate cu ajutorul cărora accesul la un sistem informatic este restrictionat sau interzis pentru anumite categorii de utilizatori*". Disponible en http://legislatie.just.ro/public/detaliidocument/71822, consultado el 11 de octubre de 2016.

protección puede extenderse al local en que se encuentra el sistema concluyendo, en relación con el Código italiano, que el tipo se refiere expresamente a las medidas de seguridad que condicionen el acceso al sistema, y no al local en que se ubica[555], razón por la cual no debe realizarse una interpretación extensiva.

En cualquier caso, habrá que valorar las circunstancias en cada caso para comprobar si la medida de seguridad establecida estaba específicamente orientada a impedir el acceso al sistema, excluyendo del concepto aquellas que no vengan referidas de forma individualizada al citado acceso, a efectos de evitar una interpretación excesivamente amplia del tipo. Como indica MORALES GARCÍA el nivel de seguridad no es un elemento que pueda describirse en el tipo, sino que deberá establecerse en relación con el estado de la técnica del momento y los usos y costumbres del lugar[556]. Se evidencia así el empleo de un elemento normativo social o cultural por el legislador en la redacción del tipo.

Por otra parte, si para que el acceso al conjunto o una parte de un sistema de información sea típico es necesario que tenga lugar "*vulnerando las medidas de seguridad establecidas para impedirlo*". Esto supone que, tal y como mantienen ANARTE BORRALLO y DOVAL PAIS[557], si un sistema informático tiene sus puertas abiertas

---

555 PECORELLA, C., "El acceso abusivo a los sistemas ...", *cit*., nota 434, p. 272.

556 MORALES GARCÍA, O., "Delincuencia informática ...", *cit*., nota 142, p. 187.

557 ANARTE BORRALLO, E. y DOVAL PAIS, A., "Delitos contra la intimidad ...", *cit*., nota 166, p. 456.

(no tiene antivirus, antispam, antiespía, cortafuegos, etc.), no estaremos ante los ataques típicos del artículo 197 *bis* 1. En la práctica se planteará si son adecuadas las medidas de seguridad establecidas para impedir tales conductas (actualización de antivirus, p.ej.), para lo cual deberá estarse de nuevo al estado de la técnica y a los usos y costumbres del lugar, equiparando MORALES GARCÍA las medidas de seguridad a una puerta cerrada que sólo puede ser abierta por quienes disponen de la llave de forma legítima, de igual modo que en un domicilio físico[558]. Las medidas de seguridad serían la forma en la que el sujeto pasivo del delito fija el vínculo de su sistema de información con las "esferas de reserva"[559].

Por último, al ser un delito de resultado y requerirse el acceso al conjunto o una parte de un sistema de información, como indica HURTADO ADRIÁN[560] será posible que el sujeto no consiga saltarse las medidas pese a su intención de hacerlo y haber iniciado la acción, produciéndose la tentativa inacabada, o que habiendo sido capaz de saltarlas, no pueda acceder al sistema, dando lugar a la tentativa acabada, tal y como veremos en el epígrafe 5.

Por todo ello, entiendo como medidas de seguridad aquellas aplicaciones o herramientas, incluso de naturaleza física y no sólo

---

558 En este sentido, MORALES GARCÍA, O., "Comentario a los delitos informáticos …", *cit*., nota 437, p. 157.

559 MORALES GARCÍA, O., "Delincuencia informática …", *cit*., nota 142, p. 187.

560 HURTADO ADRIÁN, A., "Accesos informáticos ilícitos …", *cit*., nota 145, p. 130.

informáticas, establecidas específicamente para impedir el acceso, por cuanto ponen de manifiesto que el titular ha constituido medios para impedir el libre acceso a su domicilio informático, tratando de evitar intrusiones no autorizadas y salvaguardando así la seguridad del sistema. Obviamente, esta consideración no debe entenderse en un sentido tan amplio que pueda comprender casos como el citado y rechazado por PECORELLA, relativo a medidas para impedir el acceso a un local donde se encuentra el sistema, sino que deben ser fijadas con el fin concreto de impedir el *hacking*[561]. Esto llevará a una labor interpretativa en cada supuesto, excluyendo las que no vengan referidas de forma individualizada al acceso, evidenciándose el empleo de un elemento normativo social o cultural por el legislador, por cuanto como señala MORALES GARCÍA[562], habrá que atender al estado de la técnica, usos y costumbres del lugar.

### *2.2.3 El concepto de no "estar debidamente autorizado".*

La falta de autorización fue introducida por la LO 5/2010 en el anterior artículo 197.3, si bien tras la LO 1/2015 se ha optado en el artículo 197 *bis* 1 por el término "*sin estar debidamente autorizado*" sustituyendo a la anterior mención a que "*acceda sin autorización"*.

[561] PECORELLA, C., "El acceso abusivo a los sistemas ...", *cit*., nota 434, p. 272.

[562] MORALES GARCÍA, O., "Delincuencia informática ...", *cit*., nota 142, p. 187.

Esta modificación parece acertada en la medida en que la mera referencia a "*sin autorización*" introducida con la reforma de la LO 5/2010, podía conllevar numerosos problemas de interpretación. En este sentido, en referencia a las tres conductas de los apartados 1, 2 y 3 del anterior artículo 197 y al acceso sin autorización, TOMÁS VALIENTE-LANUZA planteaba el supuesto del acceso a datos sobre la salud de una persona (p.ej. marcadores de VIH) sin su conocimiento, a partir de la inicial muestra orgánica que sí había autorizado, caso en el que, conforme a la anterior redacción, la conducta sería atípica a pesar de verse afectada la intimidad[563].

La falta de autorización dota de relevancia penal a la conducta, por encontrarnos en el campo de la confidencialidad (HURTADO ADRIÁN). De esta forma, según resulta de lo expuesto en el subepígrafe anterior, el hecho de que existan medidas de seguridad, estando por tanto el sistema protegido, evidencia que el titular no quiere que se acceda y, en consecuencia, saltarlas a sus espaldas incidirá en la falta de autorización[564].

El legislador nacional no se ha ocupado de introducir una definición al respecto como la establecida en el artículo 1.d) de la DM 2005/222/JAI, donde se declara:

"*A los efectos de la presente Decisión marco se entenderá por:*

563 TOMÁS-VALIENTE LANUZA, C., "Título X. Delitos contra la Intimidad ...", *cit*., nota 127, p. 798.

564 HURTADO ADRIÁN, A., "Accesos informáticos ilícitos ...", *cit*., nota 145, p. 128.

*(...) d) «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*".

Definición similar a la contenida en la legislación chipriota, en la que se abarca el acceso o intromisión no autorizada por el propietario o titular de otro derecho sobre el sistema informático o una parte del mismo o prohibidos por las disposiciones de esta Ley[565].

Desde un punto de vista gramatical, "*autorizar*", conforme a la definición de la RAE, se entiende como "*dar o reconocer a alguien facultad o derecho para hacer algo*"[566].

Respecto a la autorización, en materia de intromisión en la esfera de la intimidad, la STC 196/2004 declaraba la nulidad del despido de una trabajadora de IBERIA por haberse practicado sobre la base de un análisis de orina en el que le fue detectado el consumo de cannabis. Esta Sentencia concluía que se había vulnerado la intimidad de la trabajadora por cuanto no se contaba con la habilitación legal, ni con su consentimiento eficaz, ni con la información expresa y previa por parte de IBERIA sobre este punto, considerando que "*se vulnera el derecho a la intimidad personal cuando la actuación sobre su ámbito propio y reservado no sea acorde con la Ley y no sea consentida, o cuando, aun autorizada, subvierta los términos y el alcance para el que se otorgó el consentimiento, quebrando la*

565 *Vid., supra* epígrafe 2.1 del Capítulo II.

566 Definición disponible en http://lema.rae.es/drae/?val=autorizar, consultado el 17 de septiembre de 2015.

*conexión entre la información personal que se recaba y el objetivo tolerado para el que fue recogida".* Además, se consideraba necesario tener en cuenta la información que debía darse al sujeto al que se le va a practicar este tipo de pruebas, por cuanto *"el acto de libre determinación que autoriza una intervención sobre ámbitos de la intimidad personal, para ser eficaz, requiere que el trabajador sea expresamente informado de las pruebas médicas especialmente invasoras de su intimidad. Esa exigencia significa que el trabajador debe recibir información expresa, al tiempo de otorgar su consentimiento, sobre cualquier prueba o analítica que pudiera llegar a afectar a su intimidad corporal (…) la misma necesidad de información previa existe cuando las pruebas a practicar sean ajenas a la finalidad normativa de vigilancia de la salud en relación con los riesgos inherentes al trabajo*", concluyendo la Sentencia declarando que "*Iberia, LAE, SA, tenía la obligación de informar expresamente a la trabajadora de esa analítica concreta, toda vez que, si bien no afectaba a la intimidad corporal, según se dijo, sí tenía como objeto datos sensibles que lo imponían*"[567]. Esto supone la necesidad de una información previa al consentimiento para llevar a cabo la intromisión en la intimidad, porque en caso contrario no puede entenderse que exista consentimiento y la intervención vulneraría ese bien jurídico.

La nueva redacción del artículo 197 *bis* 1 parece que zanja esta polémica y exige una autorización "debida", lo que implica que sea

[567] STC 196/2004, de 15 de noviembre de 2004, Recurso de Amparo núm. 1322/2000, Pte. Excmo. Sr. D. Francisco Javier Delgado Barrio (RTC 2004\196), FJ 9 y 10.

necesario un consentimiento indubitado, expreso o tácito, para poder acceder al sistema de información. Así, en la tanto el Tribunal Supremo como el Tribunal Constitucional han admitido el consentimiento tácito para el acceso a la intimidad, considerándose en la STS de 24 de febrero de 2015 que el ordenador es un "*medio idóneo para el ejercicio de la intimidad personal, resultando entonces necesario para acceder a su contenido el consentimiento de su titular o que se den los presupuestos que legalmente habilitan la intromisión*"[568]; en la STC 196/2004, en relación con la práctica de pruebas médicas, que "*ni la Constitución impone como requisito del consentimiento, la forma escrita. Bastará, en principio, desde la perspectiva constitucional, que quepa verificar la voluntad real de someterse a la prueba médica, lo que en absoluto excluye la eficacia del consentimiento verbal o incluso la de la realización de actos concluyentes que expresen dicha voluntad*"[569]; o la STC 22/1984, en relación con la inviolabilidad del domicilio, en su FD 3º, "*En el texto constitucional, la norma de interdicción de entrada y de registro sólo admite unas excepciones muy determinadas: el consentimiento del titular, que según el texto del precepto no necesita ser expreso*"[570].

Por tanto, el criterio anterior evidencia que deberá existir una información dirigida a llevar a cabo la intervención en ese ámbito del

---

568 STS de 24 de febrero de 2015, *cit*., nota 83, FD 4º.

569 STC de 15 de noviembre de 2004, *cit*., nota 561, FD 9º.

570 STC 22/1984, Sala 2ª, de 17 de febrero de 1984, recurso 59/1983, Pte. Excmo. Sr. D. Luis Díez-Picazo y Ponce de León (EDJ 1984/22), en relación con la inviolabilidad del domicilio, en su FD 3º.

sujeto pasivo y el consentimiento que se otorgue podrá ser expreso o tácito, pero no debe quedar duda de su existencia, sin que la mera falta de oposición del titular pueda considerarse *per se* una autorización tácita para el acceso, por cuanto tal y como declaraba la STC 209/2007 en relación con la autorización para la entrada a un domicilio "*es preciso el consentimiento de su titular para justificar la intromisión domiciliar ex art. 18.2 CE, no bastando su falta de oposición a la misma, por mucho que en determinados contextos la falta de oposición pueda ser indiciaria de la concurrencia de un consentimiento tácito*"[571]. En este sentido, el artículo 2.1 de la DM 2005/222/JAI se refiere a estas conductas con "*el acceso intencionado sin autorización*", y el artículo 3 de la Directiva 2013/40/UE a que se haya realizado "*el acceso sin autorización*", por lo que resulta evidente que también para el legislador europeo la autorización debe existir, lo que excluye los supuestos de falta de oposición del titular para el acceso al sistema.

Por otra parte, para ANARTE BORRALLO y DOVAL PAÍS, la referencia del artículo 197 *bis* 1 a "*debidamente*" llama la atención sobre la legitimidad de la competencia de la persona autorizante o la

[571] Así lo declaraba, en relación con la autorización para la entrada a un domicilio, la STC, Sala 1ª, de 24 de septiembre de 2007, nº 209/2007, recurso 6377/2005, Pte. Excma. Sra. Dª María Emilia Casas Baamonde (EDJ 2007/174423), en su FD 5º: "*es preciso el consentimiento de su titular para justificar la intromisión domiciliar ex art. 18.2 CE, no bastando su falta de oposición a la misma, por mucho que en determinados contextos la falta de oposición pueda ser indiciaria de la concurrencia de un consentimiento tácito*".

fuente de la autorización[572]. Se plantea aquí la duda de si el legislador debería haberse molestado en establecer una edad mínima para otorgar esa autorización debida para el acceso, como sí ha detallado en el artículo 13 del Reglamento de la LOPD. Este precepto dispone que:

"*Podrá procederse al tratamiento de los datos de los mayores de catorce años con su consentimiento, salvo en aquellos casos en los que la Ley exija para su prestación la asistencia de los titulares de la patria potestad o tutela. En el caso de los menores de catorce años se requerirá el consentimiento de los padres o tutores*".

Esto ha motivado que RUEDA MARTÍN haya defendido la introducción de un nuevo apartado en el artículo 197 con el siguiente tenor: *"En los delitos contra la intimidad y la propia imagen cometidos a través de cualquier tecnología de la información y de la comunicación, el consentimiento de un menor de edad tendrá relevancia cuando éste tenga más de catorce años*". A partir de esa edad, la capacidad del menor para otorgar un consentimiento eficaz y excluir la tipicidad va a depender de su grado de madurez para la comprensión del alcance y trascendencia de la decisión, considerando el interés superior del menor y con carácter restrictivo[573].

---

572 ANARTE BORRALLO, E. y DOVAL PAIS, A., "Delitos contra la intimidad ...", *cit*., nota 380, p. 513.

573 RUEDA MARTÍN, M. A., "La relevancia penal del consentimiento del menor de edad en relación con los delitos contra la intimidad y la propia imagen (especial consideración a la disponibilidad de la propia imagen del menor de edad en el ciberespacio)", en *Indret*, Barcelona, octubre de 2013,

Por tanto, respecto a la posibilidad de que un menor o un incapaz puedan autorizar debidamente a un tercero para acceder al sistema de información, habría sido deseable que el legislador hubiese establecido una edad mínima para poder otorgar ese consentimiento debido[574].

Ante el silencio legislativo, será necesario un esfuerzo interpretativo. Así, tal y como señalan ANARTE BORRALLO y DOVAL PAÍS en relación con el nuevo delito contra la intimidad del artículo 197.7 CP, relativo a la revelación de imágenes obtenidas con anuencia del titular, la incapacidad absoluta para consentir conllevará la falta de anuencia[575] y, en los restantes supuestos, siguiendo a LLORIA GARCÍA, deberán considerarse las peculiaridades de cada caso, los riesgos que contiene ese consentimiento y la comprensión por parte de quien lo otorga, argumentos que parecen trasladables igualmente al debido consentimiento para acceder a un sistema de información, dada la ubicación del precepto entre los delitos contra la intimidad[576].

---

disponible en http://www.raco.cat/index.php/InDret/article/view/270185/357761, consultado el 15 de octubre de 2016, p. 32.

574 ANARTE BORRALLO, E. y DOVAL PAIS, A., "Delitos contra la intimidad ...", *cit*., nota 380, p. 529.

575 ANARTE BORRALLO, E y DOVAL PAIS, A., "Efectos de la reforma de 2015 en los delitos contra la intimidad", en Diario La Ley, nº 8744, 19 de abril de 2016, p. 3.

576 LLORIA GARCÍA, P., "Menores, redes sociales e intimidad: consentimiento y tutela. Algunas consideraciones", en ANARTE BORRALO, E., MORENO MORENO, F. y GARCÍA RÚIZ, C. (Coordinadores), *Nuevos*

En principio, el acceso autorizado podrá provenir del propietario del sistema o del titular legítimo[577] y el consentimiento otorgado determinará los límites del acceso, alcance y objetivos a los efectos del acceso, de tal forma que tal y como se reitera en la jurisprudencia y la doctrina constitucional, la intimidad del sujeto quedará vulnerada cuando la conducta de acceso al ámbito reservado "*aun autorizada, subvierta los términos y el alcance para el que se otorgó el consentimiento, quebrando la conexión entre la información personal que se recaba y el objetivo tolerado para el que fue recogida*"[578] y ese consentimiento podrá ser revocado en cualquier momento[579].

---

*conflictos sociales ...*, *cit*., nota 340, p. 255.

577 PICOTTI, L., "National legislation implementing the Convention on Cybercrime – Comparative analysis and good practices", en *Council of Europe*, 24 de agosto de 2008, consultado el 11 de octubre de 2016 en https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802fa3bc.

578 STC de 15 de noviembre de 2004, *cit*., nota 561, en su FD 2º, la STC, Sala 1ª, de 24 de septiembre de 2007, nº 206/2007, recurso 4487/2005, Pte. Excmo. Sr. D. Manuel Aragón Reyes (EDJ 2007/158668) en su FD 5º, o la STC, Sala 1ª, de 23 de marzo de 2009, nº 70/2009, recurso 2826/2004, Pte. Excma. Sra. Dª María Emilia Casas Baamonde (EDJ 2009/50401), en su FD 2º.

579 Así, con ocasión de los datos relativos a la salud de una persona, la STC, Sala 2ª, de 29 de junio de 2009, nº 159/2009, recurso 9914/2006, Pte. Excmo. Sr. D. Vicente Conde Martín de Hijas (EDJ 2009/150475), después de declarar en su FD 3º que "*la información relativa al estado de salud de una persona forma parte de este reducto de privacidad que garantiza el art. 18.1 CE, conviene señalar la existencia de límites respecto al carácter secreto de los datos relativos a la salud que determinan que, en su caso, no toda injerencia o afectación de este derecho resulta ilegítima*", se concluye que "*la afectación no será ilegítima cuando medie el previo consentimiento*

Así, si bien en relación con el *sexting* y considerando que en este caso el consentimiento debe ser expreso, LLORIA GARCÍA indica que cuando se trata de un acto íntimo, el autorizante tiene expectativas de privacidad y que su autorización lo sea para un uso privado de sus imágenes, no para un uso público, lo que significa que el consentimiento es "no extensivo", de tal manera que si las imágenes se utilizan más allá del ámbito íntimo, queda anulado porque no se ha autorizado ese uso[580]. Este criterio del consentimiento no extensivo parece ajustado también a los casos de *hacking*, donde el titular autoriza para el acceso total o parcial de su sistema de información, por lo que también quedaría anulado más allá de los límites de esa autorización.

De igual forma, si como en el Derecho chipriota comprendemos en el acceso sin autorización también los supuestos de prohibición legal, en estos casos será la norma aplicable la que especifique esos márgenes del acceso, tal y como sucede en el acceso a los sistemas de información autorizados judicialmente en los casos legalmente previstos.

Por tanto, además de la autorización para el acceso proveniente del propietario del sistema o del titular legítimo, también es posible

---

*(eficaz) del afectado, que permite la inmisión en el derecho a la intimidad y que, lógicamente, puede ser revocado en cualquier momento (STC 196/2006, de 3 de julio, FFJJ 5 y 6)*".

580 LLORIA GARCÍA, P., "Delitos y redes sociales: los nuevos atentados a la intimidad, el honor y la integridad moral. Especial referencia al *sexting*", *La Ley Penal*, nº 105, ed. Wolters Kluwer, noviembre-diciembre 2013, p. 7.

que la autoridad judicial permita el acceso en los casos legalmente previstos. Así, en la STS de 27 de julio de 2016[581] se establece que, tal y como sucede con los otros derechos fundamentales, la inviolabilidad del domicilio o el secreto de las comunicaciones pueden estar sujetos a injerencias legítimas, "*en aras a la consecución de unas finalidades de la importancia justificativa suficiente y con estricto cumplimiento de determinados requisitos en orden a garantizar el fundamento de su motivo y la ortodoxia en su ejecución*". Precisamente, por cuanto el artículo 12 de la DUDH prohíbe las "*injerencias arbitrarias*", el artículo 17 del PIDCP proscribe las "*arbitrarias o ilegales*" y el artículo 8.2 del CEDH posibilita la injerencia por la autoridad pública cuando esté prevista por la ley "*y constituya una medida que, en una sociedad democrática, sea necesaria para la seguridad nacional, la seguridad pública, el bienestar económico del país, la defensa del orden y la prevención de las infracciones penales, la protección de la salud o de la moral, o la protección de los derechos y las libertades de los demás*". En consecuencia, tal y como matiza la citada Sentencia, el legislador y la jurisprudencia han sido muy rigurosos describiendo y vigilando los requisitos para las citadas intromisiones legítimas, "*tanto desde el punto de vista del debido respeto al derecho fundamental en sí mismo, cuya infracción podría constituir incluso un verdadero delito, como del de la eficacia y valor procesal que a los resultados obtenidos con su práctica pudiera, en cada caso,*

[581] STS, Sala 2ª, de 27 de julio de 2016, nº 693/2016, recurso 10896/2015, Pte. Excmo. Sr. D. José Manuel Maza Martín (EDJ 2016/113593), FD 3º.

*otorgárseles*". En este sentido, recuerda que para la validez probatoria de la información obtenida como consecuencia de las intervenciones, es necesario que la intromisión se lleve a cabo con la citada autorización judicial, "*es decir, que sean autorizadas y, ulteriormente, controladas por la Autoridad judicial"*; la especialidad "*en el sentido de que tales diligencias han de ser acordadas con motivo de unas concretas actuaciones llevadas a cabo para la investigación de unos hechos aparentemente delictivos"*; la proporcionalidad de la injerencia en un derecho fundamental; la necesidad, en cuanto "*acudir a semejante medio de investigación, dadas las características de los hechos investigados y la grave dificultad para su descubrimiento por otros mecanismos"*; y la suficiencia en la motivación de la decisión judicial, lo cual supone *"reflejar la existencia de los anteriores requisitos"*.

Estos requisitos, en principio previstos para la inviolabilidad del domicilio o el secreto de las comunicaciones, también parecen aplicables para que sea válido el consentimiento judicial para el acceso a un sistema informático.

De forma más específica respecto a la autorización judicial para el acceso al sistema informático, tras la LO 13/2015, se encuentran en el Capítulo IV de la LECrim las denominadas "pruebas tecnológicas", dedicado a las "*Disposiciones comunes a la interceptación de las comunicaciones telefónicas y telemáticas, la captación y grabación de comunicaciones orales mediante la utilización de dispositivos electrónicos, la utilización de dispositivos*

*técnicos de seguimiento, localización y captación de la imagen, el registro de dispositivos de almacenamiento masivo de información y los registros remotos sobre equipos informáticos*" (artículos 588 *bis*.a y siguientes). Estos preceptos establecen la posibilidad de que la autoridad judicial permita el acceso a sistemas de información durante la instrucción de un procedimiento, con plena sujeción a los principios de especialidad, idoneidad, excepcionalidad, necesidad y proporcionalidad de la medida (588 *bis*.a); bien de oficio o a instancia del Ministerio Fiscal o la Policía Judicial (588 *bis*.b); por auto motivado (588 *bis*.c); tramitándose la solicitud y las actuaciones en pieza separada y secreta (588 *bis*.d); con una duración que se fije, prorrogable, pero no más allá del tiempo imprescindible para esclarecer los hechos (588 *bis*.e y 588 *bis*.f); con la obligación policial de informar a la autoridad judicial sobre la medida en la forma que se determine y al concluir (588 *bis*.g); pudiendo la autoridad judicial acordar el cese en la medida cuando cesen las circunstancias que la motivaron o sea evidente que no se obtienen los resultados pretendidos (588 *bis*.j); concluyendo con la destrucción de los registros una vez se dicte resolución firme poniendo término al procedimiento (588 *bis*.k).

Por otro lado, se ha entendido que en el acceso policial al sistema informático no es suficiente con la resolución judicial previa que autorice para acceder al domicilio donde se encuentran los dispositivos, sino que es necesario un razonamiento judicial para autorizar el sacrificio de los derechos que el acceso al sistema

informático conlleva. Este es el criterio mantenido por el Tribunal Supremo en su Sentencia de 24 de febrero de 2015[582], por cuanto "*tanto desde la perspectiva del derecho de exclusión del propio entorno virtual, como de las garantías constitucionales exigidas para el sacrificio de los derechos a la inviolabilidad de las comunicaciones y a la intimidad, la intervención de un ordenador para acceder a su contenido exige un acto jurisdiccional habilitante. Y esa autorización no está incluida en la resolución judicial previa para acceder al domicilio en el que aquellos dispositivos se encuentran instalados. De ahí que, ya sea en la misma resolución, ya en otra formalmente diferenciada, el órgano jurisdiccional ha de exteriorizar en su razonamiento que ha tomado en consideración la necesidad de sacrificar, además del domicilio como sede física en el que se ejercen los derechos individuales más elementales, aquellos otros derechos que convergen en el momento de la utilización de las nuevas tecnologías".*

No obstante, en este caso el acusado había sido puesto en libertad y fue entonces cuando los agentes le solicitaron autorización para estudiar su teléfono móvil, disco duro externo y *tablet*, intervenidos en el registro domiciliario, facilitando las claves de acceso a sus cuentas de *Facebook*, *Tuenti* y *Twitter* y los estudios sin objeción alguna ni necesidad de abogado para prestar consentimiento válido al estar en libertad, "*firmando la diligencia en prueba de conformidad, siendo entonces y no antes, cuando la policía realizó el*

582 STS de 24 de febrero de 2015, *cit*., nota 83, FD 4º.

*volcado de las conversaciones*" con el menor, que era el objeto de la investigación.

En este sentido, el Capítulo VIII de la LECrim, también introducido por la mencionada LO 13/2015, está dedicado al "*Registro de dispositivos de almacenamiento masivo de información*", en el que se establece expresamente la necesidad de la motivación individualizada cuando se produzca un registro domiciliario y sea previsible la aprehensión de sistemas informáticos, debiendo extenderse el razonamiento de la resolución judicial a los motivos que legitimen el acceso a la información contenida en los dispositivos. Además, la simple incautación de los dispositivos durante un registro domiciliario no autoriza el acceso a su contenido, sin perjuicio de que pueda posteriormente ser autorizado judicialmente (artículo 588 *sexies*.a). Esta previsión también es aplicable cuando los ordenadores o dispositivos de almacenamiento de datos sean aprehendidos con independencia de un registro domiciliario (artículo 588 *sexies*.b). La autorización judicial para el acceso determinará las condiciones y alcance, así como que se realicen copias de los datos y las medidas para garantizar la integridad de los datos y su conservación, evitando en la medida de lo posible la incautación de los soportes que contengan datos o archivos informáticos cuando puedan causar grave perjuicio al titular o propietario y se pueda obtener una copia, salvo que constituyan objeto o instrumento del delito (artículo 588 *sexies*.c).

No obstante, de conformidad con el artículo 588.*sexies*.4 de la citada ley procesal, en los supuestos de urgencia es posible que la

Policía Judicial acceda a los datos, en lo que constituye un supuesto de acceso al sistema sin autorización judicial previa, cuando sea imprescindible la adopción de la medida. En estos casos puede accederse a los datos contenidos en el dispositivo, si bien existe la obligación policial de comunicar inmediatamente y por escrito motivado, en el plazo de veinticuatro horas, las razones de la adopción de la medida, la actuación y su resultado, siendo posteriormente confirmada o revocada por el Juez competente en el plazo de setenta y dos horas. Además, según el mismo precepto, es posible que los encargados de la investigación ordenen a cualquier persona que conozca el funcionamiento del sistema informático o sus medidas de protección, que facilite la información necesaria, obligación que no será aplicable al investigado, a las personas dispensadas de declarar por parentesco y las que estén amparadas por el secreto profesional.

Con la LO 13/2015 también se han previsto los "*Registros remotos sobre equipos informáticos*" (Capítulo IX de la LECrim), de tal forma que para la investigación de los delitos cometidos en el seno de organizaciones criminales, terrorismo, delitos cometidos contra menores o personas con capacidad modificada judicialmente y delitos contra la Constitución, de traición y relativos a la defensa nacional, se podrá autorizar judicialmente la utilización de datos de identificación y códigos, así como la instalación de un *software*, que permitan, de forma remota y telemática, el examen a distancia y sin conocimiento de su titular o usuario del contenido de un sistema informático. En estos casos, la autoridad judicial deberá concretar el sistema

informático o parte del mismo, el alcance de la medida, los agentes autorizados, la autorización para la copia de los datos y su conservación y las medidas para su conservación (artículo 588 *septies*.a), existiendo igualmente un deber de colaboración con los agentes por parte de los prestadores de servicios, titulares y responsables del sistema informático (artículo 588 *septies*.b) y con una duración máxima de la medida de un mes (artículo 588 *septies*.c).

Por otra parte, respecto al elemento de la autorización que nos ocupa, se deberá considerar que con la regulación del delito se excluyen a los protocolos de comunicación en red como las *cookies*, entendidas siguiendo a ORTS BERENGUER y ROIG TORRES[583] como bloques de datos que determinados sitios *web* envían a las máquinas que se conectan con ellos, quedando almacenadas en su disco duro. Cuando el usuario vuelve a visitar ese sitio, los datos se reenvían al servidor facilitándole información actualizada sobre el mismo: datos personales, dirección de correo electrónico, frecuencia de visitas a páginas *web*, etc. De tal forma que, como señala MIRÓ LLINARES[584], son archivos que almacenan información del usuario en su propio sistema y que sirven para que las *websites* identifiquen al visitante.

Por ello, las *cookies* no quedarían incluidas en estos casos ya que solicitan autorización y los navegadores pueden impedir o

583 ORTS BERENGUER, E. y ROIG TORRES, M., *Delitos informáticos y delitos comunes ...*, *cit*., nota 112, p. 175.

584 MIRÓ LLINARES, F., *El cibercrimen ...*, *cit*., nota 8, p. 302.

restringir estos accesos al sistema del usuario y será el usuario quien autorice o no su instalación en su sistema. Obviamente, no puede considerarse conducta autorizada a los efectos de la comisión del delito las que conllevan un exceso en la autorización recibida, como sucede con las *cookies* que incorporan virus, que suponen programas o secuencias de instrucciones y rutinas creadas con el único objetivo de alterar el correcto funcionamiento del sistema y, en la mayoría de los casos, corromper o destruir parte o la totalidad de los datos almacenados en discos duros o disquetes[585], o las que incorporan *spyware*, entendido como un virus que capturan información de los sistemas informáticos o *software* que se instala en el sistema y recopila determinada información que envía a otro sistema[586].

Por último, la falta de consentimiento no se puede presumir. En el ámbito procesal rige el principio *in dubio pro reo*, lo que implica que el que acuse deberá acreditar que no existe la debida autorización, aunque también es suficiente el reconocimiento por parte del sujeto que haya llevado a cabo el acceso no consentido. Así fue declarado en la SAP de Girona, de 22 de septiembre de 2014[587] en relación con la falta de autorización para acceder al *Facebook* de la denunciante, prueba que en el caso enjuiciado vino dada "*por la lectura que se hizo en el juicio oral, a instancias de la acusación pública y como*

585 ORTS BERENGUER, E. y ROIG TORRES, M., *Delitos informáticos y delitos comunes …*, *cit*., nota 112, p. 182.

586 Definición ofrecida por MIRÓ LLINARES, F., *El cibercrimen …*, *cit*., nota 8, p. 308.

587 SAP de Girona, Sección 4ª, de 22 de septiembre de 2014, nº 504/2014, Pte. Ilmo. Sr. D. Adolfo García Morales (JUR 2015\43164), FJ 1º.

*respuesta al silencio del acusado, amparado por su derecho fundamental a no declarar, de la declaración que hizo en instrucción, en donde, entre otras cosas, dijo "que Rafaela no le dio consentimiento para que entrara en su Facebook".*

Así pues, considero que el consentimiento tiene que ser debido tras la reforma de la LO 1/2015 y, por tanto, indubitado. Y podrá ser tanto expreso como tácito, pero en cualquiera de los casos debe existir, al constituir su ausencia un elemento esencial en la conducta de *hacking*, tanto en la normativa internacional como en el artículo 197 *bis* 1 del CP. Además, puesto que el legislador no se ha pronunciado sobre la capacidad para otorgarlo, como sucede en los delitos contra la intimidad, la autorización para el acceso al sistema informático deberá analizarse en cada caso, atendiendo a la capacidad de comprensión del sujeto y los riesgos de su otorgamiento, y podrá otorgarse por el propietario del sistema o el titular legítimo. Esa autorización delimitará el acceso consentido, siendo revocable en cualquier momento. De igual manera también será posible la autorización judicial para acceder, al estar prevista en nuestro ordenamiento procesal penal, para lo cual deberá estarse a los casos legalmente previstos en esa normativa.

### *2.2.4 Los elementos delimitadores de facilitar el hacking en el artículo 197 bis 1 en relación con las conductas del nuevo artículo 197 ter.*

Una de las novedades introducidas con la LO 1/2015 son las conductas incluidas en el nuevo artículo 197 *ter*, consistentes en producir, adquirir para su uso, importar o facilitar a terceros, con la intención de facilitar la comisión del delito de *hacking*, programas o contraseñas sin autorización[588], supuestos que traen causa del artículo 7 de la Directiva 2013/40/UE[589].

---

[588] El artículo 197 *ter* introducido por la LO 1/2015 dispone: "*Será castigado con una pena de prisión de seis meses a dos años o multa de tres a dieciocho meses el que, sin estar debidamente autorizado, produzca, adquiera para su uso, importe o, de cualquier modo, facilite a terceros, con la intención de facilitar la comisión de alguno de los delitos a que se refieren los apartados 1 y 2 del artículo 197 o el artículo 197 bis: a) un programa informático, concebido o adaptado principalmente para cometer dichos delitos; o b) una contraseña de ordenador, un código de acceso o datos similares que permitan acceder a la totalidad o a una parte de un sistema de información".*

[589] El artículo 7 de la Directiva 2013/40/UE, bajo la rúbrica "*Instrumentos utilizados para cometer las infracciones*", establece: "*Los Estados miembros adoptarán las medidas necesarias para garantizar que la producción intencional, venta, adquisición para el uso, importación, distribución u otra forma de puesta a disposición de los siguientes instrumentos, sin autorización y con la intención de que sean utilizados con el fin de cometer cualquiera de las infracciones mencionadas en los artículos 3 a 6, sea sancionable como infracción penal, al menos en los casos que no sean de menor gravedad: a) un programa informático, concebido o adaptado principalmente para cometer una infracción de las mencionadas en los artículos 3 a 6; b) una contraseña de ordenador, un código de acceso*

En principio es destacable, siguiendo a ANARTE BORRALLO y DOVAL PAÍS[590] que la técnica legislativa empleada en el artículo 197 *ter* CP resulta contraria a la seguridad jurídica y a la subsidiariedad de la intervención penal. Esto se evidencia en el empleo de expresiones como "*facilite a terceros, con la intención de facilitar la comisión de alguno de los delitos"* y el vínculo de antijuridicidad que se plantea entre el hecho y el acto preparatorio, de una parte, y el delito contra la intimidad o contra el sistema de información por otra, conexión que se produce desde el punto de vista subjetivo en la medida que se requiere actuar "*con la intención de facilitar la comisión de alguno de los delitos a que se refieren los apartados 1 y 2 del artículo 197 o el artículo 197 bis*". Todo ello evidencia en palabras de estos autores "*la escasa solidez de la intervención penal en este terreno y cuestiona, en consecuencia su legitimidad*".

Los verbos utilizados por el legislador, en relación con los instrumentos que se van a mencionar, se refieren, siguiendo la definición de CASTELLÓ NICÁS[591] a:

(i) producir, que significa crear el propio sujeto el programa, contraseña, código o datos similares para

---

*o datos similares que permitan acceder a la totalidad o a una parte de un sistema de información*".

590 ANARTE BORRALLO, E. y DOVAL PAIS, A., "Delitos contra la intimidad ...", *cit*., nota 380, p. 525.

591 CASTELLÓ NICÁS, N., "Delitos contra la intimidad ...", *cit*., nota 396, p. 508.

ponerlo a disposición del tercero que llevará a cabo el acceso;

(ii) adquirir para su uso, que implica que otro lo tiene en su poder o lo ha producido o creado antes, razón por la cual el que lo ha creado también sería castigado por producirlo; e

(iii) importar, que supone que la producción se ha llevado a cabo fuera de España.

Precisamente, esas conductas pueden ser confundidas con las de "*facilite el acceso*" del nuevo artículo 197 *bis* 1 analizadas en los anteriores apartados. En este sentido, parece que la peculiaridad del artículo 197 *ter* se encuentra en que se refiere a proporcionar instrumentos concretos para el acceso (un programa informático, una contraseña de ordenador, un código de acceso o datos similares a una contraseña o un código de acceso), pero precisamente esa ambigüedad en cuanto a facilitar "*datos similares*" a "*una contraseña de ordenador*" o "*un código de acceso*" puede plantear problemas de confusión en la práctica entre estos supuestos y los de facilitar el acceso previstos en el artículo 197 *bis* 1, generándose un concurso de normas que en principio se resolverá conforme al principio de especialidad del artículo 8 CP a favor del 197 *ter*, por las peculiaridades que a continuación se van a exponer, pero que en la práctica será de difícil solución atendida la redacción del artículo 197 *ter*, con alusiones a "*de cualquier otro modo, facilite a terceros*".

Por ello, se hace preciso fijar los citados conceptos a efectos de delimitar las conductas de facilitar el acceso previstas en el artículo 197 *bis* 1 y en el artículo 197 *ter* y considerar como punto de partida los medios o instrumentos a que se refiere este último artículo, dado que cuando se trate de comportamientos en los que no se hayan facilitado estas herramientas en principio nos encontraremos ante el genérico artículo 197 *bis* 1.

El precepto vuelve a hacer referencia al elemento "*sin estar debidamente autorizado*", que hemos analizado en el anterior subepígrafe, y se refiere indistintamente a producir, adquirir para el uso, importar o facilitar a terceros, "*con la intención de facilitar la comisión*" del delito de *hacking*, un programa informático, una contraseña de ordenador, un código de acceso o datos similares que permitan acceder al sistema de información. Por esos medios podemos entender:

- *"un programa informático"*, término que puede definirse conforme al artículo 96 de la LPI, como "*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*". Además, deberá estar "*concebido o adaptado principalmente para cometer*" el delito de acceso ilícito, lo cual, como indica MORALES PRATS, resulta criticable, por

cuanto supone la dificultad añadida de determinar qué programas son esos creados o adaptados para cometer el delito, no resultando nítida la delimitación del concepto[592].

- *"una contraseña de ordenador"*, que el artículo 2.c) del Reglamento de la LOPD define como "*información confidencial, frecuentemente constituida por una cadena de caracteres, que puede ser usada en la autenticación de un usuario o en el acceso a un recurso*".
- *"un código de acceso"* que, partiendo de la definición de código ofrecida por la RAE como *"cifra para formular y comprender mensajes secretos"*[593], podemos concluir que es la cifra que permite la entrada en todo o parte del sistema de información. En este caso, la diferencia entre contraseña y código de acceso, o *password* y *passcode* en términos anglosajones, se suele establecer comúnmente en que la contraseña se asocia a códigos alfanuméricos (o PIT - *Personal Identification Text*), mientras que el código de acceso se suele vincular a la utilización de algún código numérico (llamado PIN - *Personal Identification*

[592] MORALES PRATS, F., "La reforma de los delitos contra la intimidad ...", *cit*., nota 167, p. 467.

[593] Definición disponible en http://lema.rae.es/drae/?val=c%C3%B3digo, consultado el 23 de septiembre de 2015.

*Number*)[594].

- Por último, la expresión referida a los "*datos similares que permitan acceder a la totalidad o a una parte de un sistema de información*" ha sido criticada por QUERALT JIMÉNEZ, ya que según este autor no pueden existir datos similares a contraseñas o códigos de seguridad que no sean, precisamente, contraseñas o códigos de seguridad. Por tanto, la inclusión de estos casos de forma abierta se deberá tener por no puesta por innecesaria y por infringir la analogía *in malam partem*[595]. Sin embargo, atendido el hecho de que el legislador ha incluido expresamente estos supuestos para dar la mayor cobertura posible a la protección de los bienes, parece más acertado pensar que en estos casos, en la medida en que deben ser similares a programas informáticos, contraseña de ordenador o código de acceso, podemos concluir que en estos casos se debe entender que se trata de "datos informáticos". La DM 2005/222 y la Directiva 2013/40 definen esos datos como "*toda representación de hechos, informaciones o conceptos de una forma que permite*

[594] En este sentido, se ha consultado en fecha 23 de septiembre de 2015 la Wikipedia, https://es.wikipedia.org/wiki/Contrase%C3%B1a, por cuanto esta información es la misma que la contenida en otras páginas más técnicas.

[595] QUERALT JIMÉNEZ, J. J., *Derecho penal español ...*, *cit*., nota 11, p. 342.

*su tratamiento por un sistema de información, incluidos los programas que sirven para hacer que dicho sistema de información realice una función*"[596]. Tanto estos datos como la contraseña de ordenador y el código de acceso, citados en los dos puntos anteriores, se añade en el artículo 197 *ter* CP "*que permitan acceder a la totalidad o a una parte de un sistema de información*", configurándose todos ellos como medios para facilitar la comisión del delito de *hacking*.

En principio cabría pensar que la especialidad de los medios y las peculiaridades que deben concurrir en esos instrumentos para facilitar el acceso ilícito al sistema informático son los elementos que, en definitiva, van a delimitar las conductas encuadrables en el artículo 197 *ter*, quedando el artículo 197 *bis* 1 con un carácter residual, donde tendrán cabida las restantes conductas de facilitar el acceso ilícito atendida la falta de concreción de los medios en este caso y que en la práctica llevaría a pensar en supuestos en los que se suministren instrumentos de naturaleza no informática para la comisión del delito.

Sin embargo, la referencia del artículo 197 *ter* a las conductas de quien "*de cualquier modo, facilite a terceros*" alguno de los citados medios, deja poco margen para interpretar esos hipotéticos supuestos

[596] Artículo 1.b) de la DM 2005/222/JAI y artículo 2.b) de la Directiva 2013/40/UE.

del 197 *bis* 1. De hecho, siguiendo tanto a CASTELLÓ NICÁS[597] como a COLÁS TURÉGANO[598], podemos concluir como elemento diferenciador la circunstancia de que, por los motivos que se han expuesto[599], en el caso del artículo 197 *bis* 1 se requiere que se produzca el efectivo acceso al sistema por el sujeto al que se le ha facilitado, lo cual no es necesario en el supuesto del 197 *ter* al tratarse de un acto preparatorio[600]. En cualquier caso, en la mayoría de los supuestos se producirá un inadecuado solapamiento de ambas figuras delictivas[601].

Distinto será el supuesto en que se supere la preparación delictiva y el sujeto entre en la órbita de la ejecución del delito, en cuyo caso, como indica MORALES PRATS[602], el delito del artículo 197 *ter* quedará absorbido por aquél, conforme al principio de consunción del artículo 8.3 del CP, siendo un concurso aparente de leyes penales.

Por último, la redacción del precepto en relación con el *hacking* no ha estado exenta de críticas. A las ya comentadas de

---

597 CASTELLÓ NICÁS, N., "Delitos contra la intimidad ...", *cit*., nota 396, p. 509.

598 COLÁS TURÉGANO, A. "El delito de instrusismo informático ...", *cit*., nota 45, p. 224.

599 *Vid*., *supra* subepígrafe 2.2 de este Capítulo.

600 CASTELLÓ NICÁS, N., "Delitos contra la intimidad ...", *cit*., nota 396, p. 509.

601 COLÁS TURÉGANO, A. "El delito de instrusismo informático ...", *cit*., nota 45, p. 224.

602 MORALES PRATS, F., "Delitos contra la intimidad ...", *cit*., nota 489, p. 478.

ANARTE BORRALLO y DOVAL PAÍS sobre la poca solidez de la intervención penal en esta materia, o la relativa a la incongruencia político criminal que supone el hecho de que se sancione a quien programa una aplicación informática para acceder al sistema si después no se llega a iniciar la ejecución del delito de *hacking*, la de QUINTERO OLIVARES referida a la dificultad de establecer qué programas informáticos están concebidos o adaptados principalmente para cometer el delito y la manifestada por QUERALT JIMÉNEZ sobre la inclusión de "*datos similares*", se añade la relativa a la pena que acompaña a estos supuestos. Si consideramos que se trata de un acto preparatorio, entre otros, del delito de *hacking* previsto en el delito del artículo 197 *bis* 1, resulta sorprendente que la pena del artículo 197 *ter*[603] no sea menos grave que la prevista para estos supuestos, en lo que este autor denomina un dislate político-criminal y dogmático al conllevar una sanción prácticamente igual el delito medio que el delito fin[604], lo que implica una vulneración del principio de proporcionalidad. En este sentido, MORALES PRATS señala que el precepto supone un excesivo adelantamiento de la línea de intervención penal, porque se tipifican actos preparatorios que están lejos del círculo de lesividad material para el bien jurídico, además de estar delimitados por un elemento subjetivo del injusto, lo que "hace

[603] El artículo 197 *ter* establece una pena de prisión de seis meses a dos años o multa de tres a dieciocho meses, frente a la pena de prisión de seis meses a dos años que establece el artículo 197 *bis*.1 para el delito de *hacking*.

[604] QUERALT JIMÉNEZ, J. J., *Derecho penal español …, cit*., nota 11, p. 342.

más movedizos" los criterios para su delimintación típica[605].

En definitiva, considero que el precepto supone un nuevo adelantamiento de la barrera de protección de los bienes jurídicos protegidos a las "contribuciones materiales a los correspondientes delitos"[606] que, además de innecesaria dada la redacción del artículo 197 *bis* 1 CP, se presenta como inadecuada por las dificultades interpretativas que conlleva. Podemos decir que con la regulación de las conductas en el artículo 197 *bis* y *ter* CP el legislador ha rizado el rizo en su intento de cumplir con la normativa comunitaria, salvaguardar la seguridad de los sistemas y a la vez intentar abarcar todos los supuestos de facilitar el *hacking*, ampliando también los supuestos del artículo 197 *ter* a los de los apartados 1 y 2 del artículo 197, planteando todo ello los problemas interpretativos que se intuyen sucederán en la práctica para castigar estas conductas.

### *2.2.5 Los elementos delimitadores del hacking en relación con la conducta de mantenimiento en el sistema de información (artículo 197 bis).*

El mantenimiento en un sistema informático en contra de la

---

605 MORALES PRATS, F., "Delitos contra la intimidad ...", *cit*., nota 489, p. 478.

606 En palabras de ANARTE BORRALLO y DOVAL PAIS, en ANARTE BORRALLO, E y DOVAL PAIS, A., "Efectos de la reforma ...", *cit*., nota 575, p. 8.

voluntad de quien tenga el legítimo derecho a excluirlo constituye, como hemos visto, el segundo grupo de conductas previstas en el artículo 197 *bis* 1, que también estaban previstas en el anterior artículo 197.3 pero no en los instrumentos internacionales que motivaron las reformas de 2010 y 2015.

En el nuevo artículo 197 *bis* 1 se sigue estableciendo la misma referencia a que "*se mantenga en él* –"dentro del mismo" en el anterior artículo 197.3- *en contra de la voluntad de quien tenga el legítimo derecho a excluirlo*".

En estos casos, podemos hablar de un complemento a la conducta del acceso ilícito prevista en el mismo precepto, para una completa protección del bien jurídico, de tal forma que se referiría a supuestos en los que el acceso inicialmente es lícito pero se produce una permanencia en el sistema que excede de lo autorizado, puesto que si se exigiera un acceso inicial ilícito nos encontraríamos ante la primera de las conductas de este precepto, vaciando de contenido la segunda conducta de permanencia.

Existe una obligación de abandonar el sistema porque se pierde la autorización. Por tanto, como señala FERNÁNDEZ TERUELO, concurren dos circunstancias: la autorización previa al acceso y la pérdida expresa o tácita de ésta[607].

De esta forma, es precisa una voluntad contraria del titular del

[607] FERNÁNDEZ TERUELO, J. G., *Derecho Penal e Internet …*, *cit*., nota 82, p. 201.

sistema informático a que continúe el mantenimiento, retirando así el permiso inicialmente concedido[608]. Siguiendo a HURTADO ADRIÁN[609], por motivos de coherencia con la entrada en el sistema, donde no deben quedar dudas de la autorización debida, en el caso de la permanencia en el sistema deberá constar inequívocamente que ese permiso inicial ha sido retirado.

Uno de los problemas en la interpretación del artículo se encontrará en la exigencia o no de vulneración de medidas de seguridad en la permanencia en el sistema, por cuanto como indica MORALES PRATS[610], la redacción del precepto parece referirse tanto al acceso como al mantenimiento. En esta hipótesis cabe entender con este autor que, o bien es necesario saltar esas medidas, en cuyo caso se restringiría radicalmente el ámbito de incriminación, o bien que no se requiere esa vulneración en la permanencia no autorizada, supuesto en el cual se ampliaría el campo de aplicación del precepto, al precio de tensionar la propia redacción del artículo. La solución no es fácil, por cuanto el legislador no ha sido claro, y en principio se podría decir que el elemento determinante es el mantenerse en él "*contra la voluntad de quien tenga el legítimo derecho a excluirlo*" y no el de la vulneración de medidas de seguridad que, como se ha expuesto anteriormente, tendrían la función

608 GÓMEZ RIVERO, M. C. (Coord.) y VVAA, *Nociones Fundamentales ...*, *cit.,* nota 327, p. 231.

609 HURTADO ADRIÁN, A., "Accesos informáticos ilícitos ...", *cit*., nota 145, p. 130.

610 MORALES PRATS, F., "Título X. Delitos contra la intimidad ...", *cit*., nota 369, p. 485.

de impedir el acceso.

Por ello, autores como MUÑOZ CONDE[611] se refieren a que el acceso inicial legítimo se transforma en un acceso ilegítimo, precisamente porque el titular del sistema ha cancelado el permiso por cualquier motivo. En consecuencia, si la denegación del permiso va acompañada de medidas de seguridad para impedir la continuación en el acceso, por ejemplo modificando la clave, la nueva entrada dará lugar a la primera de las conductas del artículo 197 *bis* 1, es decir, al citado *hacking*.

Para HURTADO ADRIÁN estas conductas no son el reverso negativo de la comisión por acción, ya que mientras se exige que el acceso se lleve a cabo con vulneración de esas medidas, las medidas no se habrán vulnerado por quien entra en el sistema con autorización[612].

Por su parte, TOMÁS-VALIENTE LANUZA[613] con ocasión del anterior artículo 197.3, señalaba que el significado gramatical del precepto puede llevar a la conclusión errónea de que también se exige vulneración de medidas en el caso de mantenimiento en el sistema informático, por cuanto el sentido del artículo es comprender los supuestos de la entrada inicialmente permitida cuya autorización es retirada posteriormente. Esto supone, en consecuencia, la indiferencia

611 MUÑOZ CONDE, F., *Derecho Penal ...*, *cit.,* nota 109, p. 277.

612 HURTADO ADRIÁN, A., "Accesos informáticos ilícitos ...", *cit*., nota 145, p. 130.

613 TOMÁS-VALIENTE LANUZA, C., "Título X. Delitos contra la Intimidad ...", *cit*., nota 127, p. 803.

de que existieran o no medidas de seguridad.

Por otra parte, el tipo, inspirado en el artículo 615 *ter* del CP italiano, otorga argumentos a quienes defienden la existencia del domicilio informático como bien jurídico protegido, tal y como se ha expuesto en el Capítulo anterior. Según mantiene MORALES PRATS[614], éste sería un espacio de nuevo cuño donde se proyectaría "*la privacidad del individuo con facultades de admisión y exclusión de terceros*" y, además, tiene un claro paralelismo con el de allanamiento de morada previsto en el artículo 202.1 CP. En este precepto se establece:

"*El particular que, sin habitar en ella, entrare en morada ajena o se mantuviere en la misma contra la voluntad de su morador, será castigado con la pena de prisión de seis meses a dos años*".

Por estos motivos, siguiendo el planteamiento de JAREÑO LEAL[615] respecto al allanamiento de morada, la conducta de "mantenerse" en la morada, en este caso domicilio informático, constituiría la modalidad omisiva, siendo típica desde que quien tiene el legítimo derecho a excluirlo requiere al tercero para que abandone el conjunto o parte del sistema de información y el tercero exterioriza

614 MORALES PRATS, F., "Título X. Delitos contra la intimidad …", *cit*., nota 369, p. 485.

615 JAREÑO LEAL, A., "Delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio (2). Allanamiento de morada ", en BOIX REIG, J. (Dir.) y VVAA, *Derecho Penal. Parte Especial. Volumen I. La protección penal de los intereses jurídicos personales*, ed. Iustel, segunda edición, Madrid, 2016, p. 525.

claramente su voluntad de permanecer en el sistema. Uno de los problemas que se pueden plantear, igual que en el caso del mantenimiento no autorizado en la morada, se encuentra en el momento de la consumación, que es más complicado que con el acceso, por cuanto debe existir un mínimo de permanencia dentro del sistema.

Tal y como expone PECORELLA[616], la permanencia abusiva en el sistema de información puede comprobarse por medio de la conexión con ese sistema que no esté justificada por la labor para la que el sujeto se instaure legítimamente. Por ello, es necesario que el sujeto, estando autorizado para el acceso, aproveche para llevar a cabo actuaciones diferentes a las que estaba legitimado, de tal manera que en los supuestos en que sean idóneas para vulnerar el interés del que tenga legítimo derecho a excluirle del sistema, se producirá la permanencia ilícita en el sistema durante el tiempo que sea necesario para llevarlas a cabo. Y cita esta autora el caso de la limpiadora a la que se confían las llaves de una casa para regar sus flores cuando no está el propietario, planteando si es abusivo el comportamiento en todos los supuestos en que se difiera en tiempo y forma de lo autorizado, como por ejemplo leer un libro o fisgonear en los armarios, concluyendo que habrá que considerar la capacidad objetiva de la conducta de lesionar el interés del titular a la intimidad de su domicilio, atendida la mayor o menor relación de confianza con la

[616] PECORELLA, C., "El acceso abusivo a los sistemas ...", *cit*., nota 434, pp. 273, 280 y 281.

persona a la que se ha autorizado para la entrada del domicilio, ejemplo que sería trasladable al caso de la permanencia en el sistema por parte de la persona a la que se ha autorizado para una tarea determinada.

Parece por tanto, que la determinación de ese momento deberá individualizarse en cada caso, acreditando el momento hasta el cual el tercero fue autorizado a permanecer, la capacidad objetiva para lesionar el interés de la persona que tenga el legítimo derecho de excluirle, y todos estos problemas interpretativos además dificultarán la existencia de tentativa en esta modalidad.

Por otra parte, no se exigen ulteriores conductas al citado mantenimiento en el sistema, que serían ajenas al tipo.

Tal y como señala CASTELLÓ NICÁS[617], atendida la tendencia punitiva del legislador, no se entiende que para este segundo grupo de conductas no se haya previsto el castigo del hecho de facilitar el mantenimiento, de tal manera que mientras para el *hacking* sí que se hayan incluido las conductas de hacer posible el acceso, en el caso del mantenimiento podría haberse previsto el castigo del facilitar o permitir la permanencia en el sistema de información en contra del que tenga el derecho legítimo a excluirlo.

Según se ha expuesto en el punto anterior, el artículo 197 *ter* se refiere a todos los supuestos del artículo 197 *bis*, por tanto, a

[617] CASTELLÓ NICÁS, N., "Delitos contra la intimidad ...", *cit*., nota 396, p. 506.

posibilitar tanto el acceso como el mantenimiento por los medios que cita. Sin embargo, por su parte, el artículo 197 *bis* 1, después de tipificar las conductas de facilitar el acceso, no incluye las de hacer posible mantenimiento en el sistema de información. El planteamiento resulta inexplicable e incoherente, por cuanto parece que el legislador intentaba abarcar todos los supuestos al regular la conducta de facilitar el acceso en el mismo precepto y en el citado artículo 197 *ter* y carece de lógica que no intente comprender también en el artículo 197 *bis* 1 los casos de hacer posible el mantenimiento, más aún atendida la redacción y amplia cobertura del artículo 197 *ter*, que sí los incluye, aunque sólo a través de los instrumentos que menciona. En definitiva, si entendemos que el hecho de facilitar el acceso previsto en el 197 *bis* 1 se refiere a los casos en que efectivamente se produce ese acceso y así, como hemos visto, se distingue del 197 *ter*, y además este artículo tiene un carácter especial respecto al 197 *bis* 1, no se entiende la decisión del legislador de no haber ampliado el carácter general del artículo 197 *bis* 1 a las conductas de facilitar el mantenimiento.

Aunque según mantiene FERNÁNDEZ TERUELO[618] estas conductas pueden darse frecuentemente en el ámbito empresarial con personas o colaboradores que han prestado servicios en ella (exempleados, auditores, técnicos, etc.), parece que serán pocos los supuestos que se presenten en la práctica dado el carácter residual de esta parte del precepto, que se muestra como un complemento de la

[618] FERNÁNDEZ TERUELO, J. G., *Derecho Penal e Internet …, cit*., nota 82, p. 201.

primera conducta para una protección del bien jurídico más amplia.

Por último, como se ha expuesto anteriormente[619] siguiendo a LLORIA GARCÍA, el verbo típico y la flexibilidad o no del bien jurídico van a determinar la naturaleza permanente o no del delito, y en los delitos de peligro cabe la posibilidad de que el tipo autorice el mantenimiento de la situación de peligro por un período más o menos dilatado, a través del comportamiento descrito en la figura legal[620]. Por este motivo, suponiendo las conductas de mantenimiento una afección continuada a la seguridad del sistema informático, da lugar a su configuración como un delito permanente, es decir, una vez se permanece en el sistema de información sin autorización, la conducta persiste y se produce la continuidad del comportamiento que caracteriza a esta categoría de delitos.

### *3. POSICIÓN PERSONAL.*

#### *3.1 Planteamiento.*

Se han analizado los distintos elementos del tipo básico de *hacking*, facilitar estas conductas y el mantenimiento en los sistemas informáticos regulado en el mismo párrafo.

---

619 *Vid*., *supra* subepígrafe 2.2.1 de este Capítulo.

620 LLORIA GARCÍA, P., *Aproximación al estudio* …., *cit*., nota 541, pp. 61 y 75.

Atendiendo a la seguridad de los sistemas de información, que según se ha expuesto constituye el bien jurídico protegido en los instrumentos internacionales que motivan las reformas de 2010 y 2015 en los artículos 197.3 y 197 *bis* 1 del CP, podemos entender que en el nuevo artículo 197 *bis* 1 el acceso no autorizado a todo o parte de un sistema de información y la vulneración de las medidas de seguridad establecidas para impedirlo son los elementos que definen las conductas de *hacking*.

Por tanto, desde mi punto de vista, no parece que el legislador se haya detenido en que el sujeto tenga capacidad potencial para acceder a cualquier tipo de información que se encuentre en el sistema, requisito que sí consideraba necesario MIRÓ LLINARES[621] en su definición del *hacking* con ocasión del anterior artículo 197.3, ni tampoco que el sujeto acceda a la privacidad de los datos guardados en el sistema como indicaba MUÑOZ CONDE[622] en su definición.

Por ello, atendiendo al tenor literal del vigente artículo 197 *bis* 1 y el principio de legalidad, en nuestro Derecho penal el *hacking* es el equivalente al intrusismo informático o violación de una esfera de exclusividad del titular del sistema, siendo intrascendente el contenido del sistema, y bastando el mero acceso no autorizado al sistema de

---

621 MIRÓ LLINARES, F., "Los Delitos Informáticos ...", *cit*., nota 108, p. 145. Por otra parte, la Sentencia del Juzgado de lo Penal 2 de Barcelona, de 28 de mayo de 1999 lo define como "*un conjunto de comportamientos de acceso o interferencia no autorizados a un sistema informático o red de comunicación electrónica de datos, y a la utilización de los mismos sin autorización o más allá de lo autorizado*" (*cit*., nota 15).

622 MUÑOZ CONDE, F., *Derecho Penal ...*, *cit*., nota 109, p. 277.

información o parte del mismo vulnerando las medidas de seguridad establecidas para impedirlo, con independencia de que se acceda o no a los datos.

En consecuencia, comparto en buena parte el criterio del Juzgado de lo Penal 2 de Barcelona, en su Sentencia de 28 de mayo de 1999, al definir el *hacking* como "*un conjunto de comportamientos de acceso o interferencia no autorizados a un sistema informático o red de comunicación electrónica de datos, y a la utilización de los mismos sin autorización o más allá de lo autorizado*"[623], si bien conviene matizar que con la reforma de la LO 1/2015 no se exige ninguna utilización del sistema.

Según expone JORGE BARREIRO[624], es posible que el acceso al sistema informático no afecte a la intimidad de sujeto alguno, p.ej. cuando un sujeto salta el *baneo* en una sala de chat, que será distinto al acceso a un perfil privado creado en una red social por un sujeto, debidamente protegida y que contenga datos sensibles de ese sujeto que podrían ser utilizados por el *hacker*, razón por la cual considera razonable la interpretación restrictiva del precepto, excluyendo las conductas que sólo tangencialmente afecten a la intimidad o privacidad aunque afecte a la seguridad de los sistemas informáticos, seguridad que tiene una discutible protección penal, p.ej. cuando se accede a un chat o foro en los que no se proyecta la intimidad del

623 Sentencia del Juzgado de lo Penal 2 de Barcelona, de 28 de mayo de 1999, *cit*., nota 15, FD 1º.

624 JORGE BARREIRO, A., "Delitos contra la intimidad ...", *cit*., nota 117, p. 1044 y 1045.

titular, mientras que sí que tendrán cabida en el artículo 197 *bis* 1 los casos en los que sí esté afectada la intimidad, como sucede en el acceso al perfil de otra persona en una red social. También propone este autor otra reducción en la interpretación del precepto excluyendo los casos en que se trate del "uso normal de la red", como sucede cuando el sujeto se limita a saltarse un *baneo* en el uso normal de Internet, en el caso de que el *baneo* lo sea a la IP dinámica y reseteando la IP de su terminal o accediendo desde otro equipo a la sala de chat, siendo todo ello una posibilidad con la que cuenta el "usuario normal de Internet", como se entiende el titular del chat, y que serán casos distintos a los del uso de *keygens* o *cracks* u otros medios complejos para acceder al sistema informático y que sí que deberán ser incluidos en la interpretación del precepto.

Desde mi punto de vista, tal y como se ha expuesto en el Capitulo anterior, la consideración de la seguridad del sistema informático, comprendiendo su confidencialidad, integridad y disponibilidad, es el bien jurídico protegido, por lo que será exigible que la conducta ponga en peligro concreto alguno de estos elementos, no así la afectación a la intimidad en el modo expuesto por JORGE BARRERO. Deberá examinarse en cada caso si realmente se ha producido ese riesgo, con independencia de que como resultado también se haya producido una lesión o peligro para otro bien jurídico como pueda ser la intimidad, dando lugar en su caso a un concurso con este otro delito. Esto implica que en el ejemplo citado, va a ser irrelevante que se proyecte o no la intimidad del sujeto en el chat o

foro al que se acceda, si se ha puesto en peligro su confidencialidad, integridad o disponibilidad. Así, imaginemos que el sujeto que ha accedido al chat o foro no ha afectado a la intimidad, pero ha originado ese riesgo concreto para su seguridad, con todas las consecuencias que ello puede acarrear, por ejemplo, dejando la puerta abierta para que otro sujeto también acceda y pueda introducir un virus en el chat o foro, cometiendo un delito de daños del artículo 264 CP derivado de ese anterior acceso ilícito.

Por ello, los casos de acceso concurriendo los citados elementos pueden ser tan diversos que exigen la consideración del principio de proporcionalidad en la exégesis del artículo 197 *bis* 1 para una interpretación restrictiva, que se ajuste a las necesidades de protección considerando la intensidad del ataque y la realidad informática regulada, si bien sin llegar hasta los extremos citados por JORGE BARREIRO de excluir en esa interpretación los casos en los que el acceso no afecte a la intimidad o privacidad personal, por cuanto que no parece esa la intención del legislador en la redacción del artículo 197 *bis* 1, porque no hay que perder de vista que la seguridad de los sistemas informáticos resulta ser el bien juridico protegido por el delito de *hacking*, sin perjuicio de la tutela indirecta de otros bienes, como la citada intimidad, que se produce con el adelantamiento de las barreras de protección, tal y como se ha expuesto en el Capítulo anterior.

En cuanto a las conductas de mantenimiento en el sistema

informático, no coincido con SALVADORI[625] en la crítica a la equiparación en el mismo párrafo entre las conductas de acceso ilícito, que puede conllevar un acceso a datos y programas tal y como se regulaba en el anterior artículo 197.3, y las conductas de permanencia o parada en el sistema previo acceso lícito, que supone un peligro para los datos o programas que puedan haber en el sistema informático en cuanto puedan ser conocidos o utilizados y por tanto tan sólo implicaría un peligro indirecto para la confidencialidad e integridad del sistema informático. Aunque habría sido deseable una mayor concreción en este segundo grupo de conductas o su regulación de forma autónoma a efectos de no equipararlas con el *hacking* en sentido propio, entiendo que tanto peligro puede conllevar el acceso al sistema informático para su confidencialidad, integridad o disponibilidad, como la permanencia en él sin autorización, sin que debamos ceñirnos al efectivo acceso a datos o programas, conducta que por otra parte, caso de producirse, sería actualmente encuadrable en el apartado 1 o 2 del artículo 197.

Por último, tal y como se ha expuesto anteriormente[626], el delito de *hacking* se configura como un delito de resultado, al requerirse el acceso al conjunto o una parte de un sistema de información con su puesta en peligro, por lo que, como indica HURTADO ADRIÁN[627], será posible que el sujeto no consiga

---

625 SALVADORI, I., "Los nuevos delitos informáticos ...", *cit*., nota 106, p. 249.

626 *Vid.*, *supra* Capítulo III, epígrafe 5.

627 HURTADO ADRIÁN, A., "Accesos informáticos ilícitos ...", *cit*., nota

saltarse las medidas pese a su intención de hacerlo y haber iniciado la acción, produciéndose la tentativa inacabada, o que habiendo sido capaz de saltarlas, no pueda acceder al sistema, dando lugar a la tentativa acabada, tal y como veremos en el epígrafe 5; y además, es un delito de medios indeterminados, comprendiendo cualquier tipo de conductas que determinen el acceso. El legislador incluso ha equiparado a estos supuestos los relativos a facilitar ese acceso, dentro del mismo artículo 197 *bis* 1, o incluso facilitar el mantenimiento en el sistema por los medios o instrumentos que cita en el artículo 197 *ter*, todo ello en un evidente intento de comprender todos los casos, tanto de efectivo acceso como de facilitarlo, en la tutela de la seguridad de los sistemas informáticos.

### *3.2 Respecto al elemento de acceder a un sistema de información.*

El conjunto o parte del sistema de información se presenta como el objeto material del delito de *hacking* en nuestro Código, según hemos visto en el Capítulo anterior, y los elementos del acceso a ese sistema determinan el alcance del delito.

La tipificación del acceso a todo o parte de un sistema de información resulta más acertada para la efectiva protección de la seguridad del sistema que la limitada por el acceso a datos o

145, p. 130.

programas informáticos, en la medida que incluiría supuestos que son igualmente atentatorios contra la seguridad del sistema, como puede ser la instalación de un programa espía después de haber accedido al mismo. Además, la referencia expresa al citado objeto material, abandonando los datos o programas informáticos, deja a un lado el problema de delimitación con las conductas del artículo 197.2 CP, relativo al acceso a datos de carácter personal o familiar registrados en ficheros o soportes informáticos.

Por otra parte, la referencia a las conductas de facilitar el acceso, equiparándolas en el mismo precepto con el acceso mismo, implica poner en el mismo nivel los casos de autoría y participación. Por ello entiendo con COLÁS TURÉGANO[628] que en estos comportamientos es necesario que efectivamente se produzca el acceso, de esta forma se evita el contrasentido de castigar al que facilita la conducta de acceso como si hubiese llevado a cabo ese acceso, siendo que no se ha producido. Además, con esta interpretación también se delimitan estos supuestos con los del artículo 197 *ter*.

Comparto la postura de ANARTE BORRALLO y DOVAL PAÍS[629], las conductas se podrán llevar a cabo por cualquier medio, incluso por omisión al no estar excluida, agotándose el tipo subjetivo

---

628 COLÁS TURÉGANO, A. "Nuevas conductas delictivas ...", *cit*., nota 168, p. 676.

629 ANARTE BORRALLO, E. y DOVAL PAIS, A., "Delitos contra la intimidad ...", *cit*., nota 380, p. 518. Y ANARTE BORRALLO, E. y DOVAL PAIS, A., "Límites de la ley penal ...", *cit*., nota 24, p. 13.

con el dolo en cuanto conocimiento y voluntad de acceder o permanecer en el sistema, o facilitar el acceso, sobre todo o parte del sistema de información, sin autorización y vulnerando las medidas de seguridad establecidas para impedirlo.

Por último, no exigiendo el mero acceso al sistema informático la afección continuada a su seguridad, entiendo que nos encontraríamos ante un delito instantáneo por cuanto, una vez se accediera con la puesta en peligro para el sistema, la conducta habría finalizado y no permanecería en el tiempo, a diferencia de las conductas de permanencia en el sistema, donde precisamente el verbo típico y la flexibilidad del bien jurídico determinan en este caso la naturaleza permanente del delito, al existir la persistencia que caracteriza este tipo de delitos en tanto el sujeto se mantenga en el sistema sin autorización.

### *3.3 Las medidas de seguridad establecidas para impedirlo.*

Este elemento relacionado con el sistema de información supone la tipicidad de la conducta, de tal manera que sin medidas no hay ilícito penal y, a su vez, evidencian la voluntad del titular de no autorizar el libre acceso.

Considero que como medidas de seguridad deben entenderse todas aquellas aplicaciones o herramientas, incluso de naturaleza física y no sólo informáticas, establecidas específicamente para

impedir el acceso, por cuanto ponen de manifiesto que el titular ha constituido medios para impedir el libre acceso a su domicilio informático, tratando de evitar intrusiones no autorizadas y salvaguardando así la seguridad del sistema. Obviamente, esta consideración no debe entenderse en un sentido tan amplio que pueda comprender casos como el que rechaza PECORELLA, relativo a medidas para impedir el acceso a un local donde se encuentra el sistema, sino que deben ser fijadas con el fin concreto de impedir el *hacking*[630]. Esto llevará a una labor interpretativa en cada caso, excluyendo las que no vengan referidas de forma individualizada al acceso, evidenciándose el empleo de un elemento normativo social o cultural por el legislador, por cuanto como señala MORALES GARCÍA[631], habrá que atender al estado de la técnica, usos y costumbres del lugar.

### *3.4 No estar debidamente autorizado.*

Considero que la existencia de medidas de seguridad evidencia que existe una voluntad del titular de impedir el libre acceso, razón por la cual se hace precisa su autorización.

El citado consentimiento tiene que ser debido tras la reforma

630 PECORELLA, C., "El acceso abusivo a los sistemas ...", *cit*., nota 434, p. 272.

631 MORALES GARCÍA, O., "Delincuencia informática ...", *cit*., nota 142, p. 187.

de la LO 1/2015 y, por tanto, indubitado, sea expreso o tácito según resulta del criterio jurisprudencial y de la doctrina constitucional.

La duda se plantea desde el punto de vista de quién puede otorgarlo, porque no se establece una edad mínima en el Código Penal, que habría sido lo deseable para evitar interpretaciones extrapenales, y esto obliga a considerar las condiciones concurrentes en cada caso. Así pues, ante la falta de regulación, descartado el consentimiento del absolutamente incapaz, siguiendo a LLORIA GARCÍA[632], entiendo que deberán considerarse las peculiaridades de cada caso, los riesgos que contiene ese consentimiento y la comprensión por parte de quien lo otorga, argumentos que parecen trasladables igualmente al debido consentimiento para acceder a un sistema de información, dada la ubicación del precepto entre los delitos contra la intimidad.

Por otra parte, la autorización podrá otorgarse por el propietario del sistema o el titular legítimo, y esa autorización delimitará el acceso consentido, siendo revocable en cualquier momento. De igual manera en nuestro ordenamiento procesal penal está prevista la autorización judicial para el acceso, en los casos legalmente previstos en esa normativa.

La solicitud de autorización para el acceso, concedida por el propietario o el titular, determina la atipicidad de las denominadas *cookies*, por cuanto solicitan autorización, los navegadores pueden

632 LLORIA GARCÍA, P., "Menores, redes sociales ...", *cit*., nota 576, p. 255.

impedir o restringir estos accesos al sistema del usuario y será el usuario quien autorice o no su instalación en su sistema. Obviamente, es el usuario quien también va a delimitar hasta dónde acceden estos bloques de datos que se almacenan en su sistema.

Por último, parece evidente, por exigirlo el principio *in dubio pro reo*, que quien alegue la falta de autorización deberá probarla.

### *3.5 Elementos delimitadores de facilitar el hacking en el artículo 197 bis 1 en relación con las conductas del nuevo artículo 197 ter.*

Considero destacable, como señalan ANARTE BORRALLO y DOVAL PAÍS[633], la falta de solidez en la intervención penal empleada en el artículo 197 *ter* CP, que resulta contrario a la seguridad jurídica y la subsidiariedad del Derecho penal, usando expresiones como "*facilite a terceros, con la intención de facilitar la comisión de alguno de los delitos"* y el vínculo de antijuridicidad que se plantea entre el hecho y el acto preparatorio, de una parte, y el delito contra la intimidad o contra el sistema de información por otra, conexión que se produce desde el punto de vista subjetivo en la medida que se requiere actuar "*con la intención de facilitar la comisión de alguno de los delitos a que se refieren los apartados 1 y 2*

633 ANARTE BORRALLO, E. y DOVAL PAIS, A., "Delitos contra la intimidad …", *cit*., nota 380, p. 525.

*del artículo 197 o el artículo 197 bis*".

A ello se añade que, como apunta FRÍAS MARTÍNEZ[634] esas conductas pueden ser confundidas con las de "*facilite el acceso*" del nuevo artículo 197 *bis* 1 analizadas en los anteriores apartados.

Entiendo que la peculiaridad del artículo 197 *ter* se encuentra en que se refiere a proporcionar instrumentos concretos para el acceso, si bien la ambigüedad en cuanto a facilitar "*datos similares*" a "*una contraseña de ordenador*" o "*un código de acceso*" puede plantear problemas de confusión en la práctica entre estos supuestos y los de facilitar el acceso previstos en el artículo 197 *bis* 1. Por tanto, aunque en principio se generaría un concurso de normas que se resolverá conforme al principio de especialidad del artículo 8 CP a favor del 197 *ter*, en la práctica será difícil la delimitación, atendida la redacción del artículo 197 *ter* con alusiones a "*de cualquier otro modo, facilite a terceros*".

Por la extensión del artículo 197 *ter*, al artículo 197 *bis* 1 le quedaría un carácter residual, donde tendrán cabida las restantes conductas de facilitar el acceso ilícito atendida la falta de concreción de los medios en este caso y que en la práctica llevaría a pensar en principio tan sólo en aquellos supuestos en los que se suministren instrumentos de naturaleza no informática para la comisión del delito. Sin embargo, la referencia del artículo 197 *ter* a las conductas de quien "*de cualquier modo, facilite a terceros*" alguno de los citados

634 FRÍAS MARTÍNEZ, E., "Delitos contra la intimidad …", *cit*., nota 529, p.369.

medios, incluso deja poco margen para interpretar esos hipotéticos supuestos del 197 *bis*. De hecho, siguiendo tanto a CASTELLÓ NICÁS[635] como a COLÁS TURÉGANO[636], en estos últimos supuestos considero como elemento diferenciador la circunstancia de que en el caso del artículo 197 *bis* se requiere que se produzca el efectivo acceso al sistema por el sujeto al que se le ha facilitado, lo cual no es necesario en el supuesto del 197 *ter* al tratarse de un acto preparatorio[637]. En cualquier caso, en la mayoría de los supuestos se producirá un inadecuado solapamiento de ambas figuras delictivas.

Por último, el artículo 197 *ter* me parece criticable no sólo por los problemas de delimitación con el 197 *bis* 1, sino como señala MORALES PRATS[638], también a la hora de establecer qué programas informáticos están concebidos o adaptados principalmente para cometer el delito y la utilización de elementos demasiado abiertos como "*datos similares*", a lo que se añade la relativa a la pena que conllevan estos supuestos, por cuanto si consideramos que se trata de un acto preparatorio, entre otros, del delito de *hacking* previsto en el delito del artículo 197 *bis* 1, resulta sorprendente que la pena del artículo 197 *ter* no sea menos grave que la prevista para estos

635 CASTELLÓ NICÁS, N., "Delitos contra la intimidad ...", *cit*., nota 396, p. 509.

636 COLÁS TURÉGANO, A., "El delito de instrusismo informático ...", *cit*., nota 45, p. 224.

637 CASTELLÓ NICÁS, N., "Delitos contra la intimidad ...", *cit*., nota 396, p. 509.

638 MORALES PRATS, F., "La reforma de los delitos contra la intimidad ...", *cit*., nota 167, p. 467.

supuestos, en lo que acertadamente QUERALT JIMÉNEZ[639] denomina un dislate político-criminal y dogmático, al conllevar una sanción prácticamente igual el delito medio que el delito fin. Además, siguiendo a JORGE BARREIRO[640], me parece criticable la equiparación entre las conductas de acceso y facilitar el acceso en el mismo artículo 197 *bis* 1, por cuanto facilitar el acceso es tan genérico que puede comprender conductas de cooperación no necesaria que el legislador sitúa al mismo nivel que el propio acceso ilícito.

Por todo ello, con este nuevo adelantamiento de la barrera de protección de los bienes jurídicos al momento de facilitar las conductas del acceso, considero que era innecesario el artículo 197 *ter* atendida la existencia del 197 *bis* 1 CP, y además es inadecuado por los problemas interpretativos. Con la regulación de las conductas en el artículo 197 *bis* y *ter* CP el legislador ha rizado el rizo en su intento de cumplir con la normativa comunitaria, salvaguardar la seguridad de los sistemas y a la vez intentar abarcar todos los supuestos de facilitar el *hacking*, ampliando también los supuestos del artículo 197 *ter* a los de los apartados 1 y 2 del artículo 197, planteando todo ello una amalgama de problemas interpretativos que se intuyen sucederán en la práctica para castigar estas conductas.

---

639 QUERALT JIMÉNEZ, J. J., *Derecho penal español ...*, *cit*., nota 11, p. 342.

640 JORGE BARREIRO, A., "Delitos contra la intimidad ...", *cit*., nota 117, p. 1041.

### *3.6 Elementos delimitadores del hacking en relación con la conducta de mantenimiento en el sistema de información.*

Desde mi punto de vista, resulta evidente por motivos de coherencia con la entrada en el sistema, donde no deben quedar dudas de la autorización debida, que en el caso de la permanencia en el sistema deberá constar inequívocamente que ese permiso inicial ha sido retirado[641]. Con estas conductas ubicadas junto al acceso al sistema de información, parece que el legislador pretende una amplia tutela de su integridad y seguridad, razón por la cual y a efectos de no confundir el acceso ilícito con el mantenimiento en el sistema, entiendo acertado seguir el criterio de FERNÁNDEZ TERUELO[642], y considerar que es necesaria una autorización previa al acceso y la pérdida expresa o tácita de ésta, pues de otro modo, ante la falta de una autorización previa, nos encontraríamos ante las conductas de acceso ilícito y, por otro lado, en el caso de que no se hubiera perdido la autorización inicial, existiría un mantenimiento lícito dentro del sistema.

Atendida la redacción del artículo 197 *bis* 1, uno de los problemas en la interpretación del artículo se encontrará en la

641 En este sentido, HURTADO ADRIÁN, A., "Accesos informáticos ilícitos ...", *cit.*, nota 145, p. 130.

642 FERNÁNDEZ TERUELO, J. G., *Derecho Penal e Internet ...*, *cit*., nota 82, p. 201.

exigencia o no de vulneración de medidas de seguridad en la permanencia en el sistema. En estos casos MORALES PRATS[643] plantea como alternativas que, o bien es necesario saltar esas medidas, en cuyo caso se restringiría radicalmente el ámbito de incriminación, o bien que no se requiere esa vulneración en la permanencia no autorizada, supuesto en el cual se ampliaría el campo de aplicación del artículo, al precio de tensionar la propia redacción del artículo.

Considero que la solución no es fácil, por cuanto el legislador no ha sido claro, y entiendo que el elemento determinante es el mantenerse en él "*contra la voluntad de quien tenga el legítimo derecho a excluirlo*" y no el de la vulneración de medidas de seguridad que, como se ha expuesto anteriormente, tendrían la función de impedir el acceso, y por tanto, coincido con TOMÁS-VALIENTE LANUZA[644], que en la interpretación del anterior artículo 197.3 se refería a que el sentido del artículo es comprender los supuestos de la entrada inicialmente permitida cuya autorización es retirada posteriormente. Esto supone, en consecuencia, la indiferencia de que existieran o no medidas de seguridad.

Todo ello, por cuanto considero que, como señala MUÑOZ CONDE[645], en los supuestos de mantenimiento en el sistema el acceso inicial legítimo se transforma en un acceso ilegítimo, precisamente

---

643 MORALES PRATS, F., "Título X. Delitos contra la intimidad ...", *cit*., nota 369, p. 485.

644 TOMÁS-VALIENTE LANUZA, C., "Título X. Delitos contra la Intimidad ...", *cit*., nota 127, p. 803.

645 MUÑOZ CONDE, F., *Derecho Penal ...*, *cit*., nota 109, p. 277.

porque el titular del sistema ha retirado el permiso. En consecuencia, si la denegación del permiso va acompañada de medidas de seguridad para impedir la continuación en el acceso, por ejemplo modificando la clave, la nueva entrada dará lugar a la primera de las conductas del artículo 197 *bis* 1, es decir, al citado *hacking*. Además, como señala HURTADO ADRIÁN mientras se exige que el acceso se lleve a cabo con vulneración de esas medidas, las medidas no se habrán vulnerado por quien entra en el sistema con autorización[646].

La conducta del mantenimiento, equivaldría al mantenimiento indebido en el allanamiento de morada, conducta omisiva en este caso trasladada al sistema informático, planteándose también el problema de su consumación al requerir de una cierta permanencia temporal mínima dentro del sistema. Entiendo que ante la falta de claridad legislativa, la determinación de ese momento deberá individualizarse en cada caso, acreditando el momento hasta el cual el tercero fue autorizado a permanecer, la capacidad objetiva para lesionar el interés de la persona que tenga el legítimo derecho de excluirle y poner en peligro la seguridad del sistema, y todas estos problemas interpretativos además dificultarán la existencia de tentativa en esta modalidad.

Por otra parte, parece ilógico que el legislador se haya referido a facilitar el mantenimiento en el sistema por alguno de los medios que cita en el artículo 197 *ter* y, sin embargo, sin motivo alguno no se

646 HURTADO ADRIÁN, A., "Accesos informáticos ilícitos ...", *cit*., nota 145, p. 130.

mencionen esas conductas de facilitar la permanencia en el sistema igualmente dentro del artículo 197 *bis*, tal y como sucede con los supuestos de acceso. De esta forma se evidencia por tanto una vez más la defectuosa técnica legislativa en la duplicidad de estas conductas mencionadas en el artículo 197 *bis* y 197 *ter* CP.

A pesar de todo, considerando los argumentos manifestados, creo que las conductas incluidas en el nuevo artículo 197 *bis* 1 van dirigidas a una íntegra protección de los sistemas de información, y la nueva dicción de algunos términos está orientada a evitar problemas de delimitación con otras conductas que ya cuentan con una tipificación específica en otros preceptos.

Por último, parece que esta parte del precepto dedicada al mantenimiento en los sistemas de información va a tener poca aplicación práctica, atendida la extensión de las conductas de acceso en la nueva regulación de los citados preceptos. Es evidente que la práctica nos dirá si el alcance del artículo es lo suficientemente exhaustivo o si habría sido deseable una mayor regulación, incluyendo p.ej. otras conductas como la señalada por CASTELLÓ NICÁS[647] en referencia a las conductas de facilitar el mantenimiento.

[647] CASTELLÓ NICÁS, N., "Delitos contra la intimidad …", *cit*., nota 396, p. 506.

### *4. ASPECTO SUBJETIVO.*

Siguiendo a HURTADO ADRIÁN, se puede afirmar que la falta de autorización es lo que atribuye de relevancia penal a la conducta[648], configurándose como un delito doloso, ello, en la medida en que la DM 2005/222/JAI se refería en su artículo 2.1 al "*acceso intencionado sin autorización al conjunto o una parte de un sistema de información*", dolo que se refiere a la consciencia y voluntad de acceder sin autorización al sistema de información, vulnerando las medidas de seguridad, o mantenerse dentro del sistema en contra de la voluntad de quien tenga el legítimo derecho a excluirlo, o bien, tras la reforma de la LO 1/2015, con conocimiento y voluntad de facilitarlo.

En el caso de error acerca de estos elementos, se considerará error de tipo tal y como indica JORGE BARREIRO[649] y, por tanto, conllevará las consecuencias del artículo 14.1 CP. Este último sería el caso citado por MIRÓ LLINARES[650] de redes internas empresariales o institucionales, en las que el sujeto no se aperciba de su acceso a parte del sistema de otra persona. No obstante, según indicaba este autor, la exigencia de que se vulneren medidas de seguridad hará

---

[648] HURTADO ADRIÁN, A., "Accesos informáticos ilícitos ...", *cit*., nota 145, p. 128.

[649] JORGE BARREIRO, A., "Delitos contra la intimidad ...", *cit*., nota 117, p. 1045 y JORGE BARREIRO, A., "Delitos contra la intimidad ...", *cit*., nota 483, p. 1067.

[650] MIRÓ LLINARES, F., "Los Delitos Informáticos ...", *cit*., nota 108, p. 154.

difícil en la práctica apreciar un supuesto en el que el sujeto quebrante esas medias y no se aperciba de ello.

No obstante, conviene tener presente que tras la reforma de la LO 1/2015 también se castiga de forma alternativa, tanto al sujeto que accede como al que facilite ese acceso, por lo que podría ser más fácil pensar en el error de tipo en un sujeto que creyese que está facilitando a otro sujeto el acceso al que se considera su sistema informático, siendo que en realidad se está accediendo ilícitamente a un sistema ajeno.

Esta postura de considerar error de tipo cuando recaiga sobre alguno de los citados elementos es la mantenida también por ANARTE BORRALLO y DOVAL PAÍS[651], que se pronuncian con ocasión de la cláusula "*sin estar debidamente autorizado*", que se configura como uno de los elementos del tipo, de tal manera que si el sujeto está debidamente autorizado, el hecho es atípico, lo que conlleva que el dolo debe abarcar también su contenido y, si el sujeto incurre en error sobre la existencia de esa autorización, se trate de un error de tipo conforme al artículo 14.1 del CP[652].

Cuestión distinta será que el error recaiga sobre la ilicitud del acceso al sistema informático ajeno, en cuyo caso parece razonable

---

651 ANARTE BORRALLO, E. y DOVAL PAIS, A., "Delitos contra la intimidad ...", *cit*., nota 380, p. 514.

652 El artículo 14.1 CP dispone que "*El error invencible sobre un hecho constitutivo de la infracción penal excluye la responsabilidad criminal. Si el error, atendidas las circunstancias del hecho y las personales del autor, fuera vencible, la infracción será castigada, en su caso, como imprudente".*

considerar el error de prohibición con las consecuencias del artículo 14.3 CP[653]. En este caso resulta complicado en la práctica que puedan darse el error de prohibición en el *hacking*. Podríamos pensar en supuestos tales como el del sujeto que ignorando que no puede quebrantar la medida de seguridad establecida por un usuario de una aplicación, que precisamente la ha creado para impedir el acceso de terceros a esa aplicación con su perfil, la vulnera y accede a su perfil, no teniendo conocimiento de la antijuridicidad de su conducta.

En el delito que nos ocupa tienen cabida también los supuestos de dolo eventual, tal y como sucedería en el caso del sujeto que pretende superar la medida de seguridad de un sistema informático como reto personal, asumiendo como posible que con el quebrantamiento de esa medida se producirá el acceso al mismo con el consiguiente peligro para su confidencialidad, integridad o disponibilidad. En este sentido, como hemos visto en los epígrafes anteriores, el dolo eventual ya fue admitido en un AAP de Barcelona[654] y en relación al artículo 197.2 *in fine* CP en el acceso a una aplicación de correo electrónico ajeno y las diferentes bases de datos contenidas en el sistema, incluso sin llegar a abrir mensaje alguno, puede ser típico por cuanto supone una intromisión en la intimidad que además puede hacer posible el conocimiento de datos

653 El artículo 14.3 CP establece que "*El error invencible sobre la ilicitud del hecho constitutivo de la infracción penal excluye la responsabilidad criminal. Si el error fuera vencible, se aplicará la pena inferior en uno o dos grados".*

654 AAP de Barcelona de 22 de octubre de 2012, *cit*., nota 537, FD 2º.

reservados. Todo ello, sin perjuicio de que además nuestro Código Penal establece un sistema de *numerus clausus* en cuanto a delitos imprudentes (artículo 12 CP), no estando tipificada la modalidad imprudente en el delito de *hacking*, de tal manera que, como señala COLÁS TURÉGANO[655], el hecho será atípico si el acceso se ha producido por un descuido o negligencia.

En cualquier caso será irrelevante la finalidad perseguida por quien accede o se mantiene en el sistema siguiendo a PECORELLA[656] en referencia al artículo 615 *ter* del CP italiano, argumento que resulta trasladable a nuestro ordenamiento atendido el paralelismo que hemos visto anteriormente entre ese precepto y el artículo 197 *bis* 1 CP. Al respecto, el Tribunal de Casación italiano, Sección Conjunta, en su Sentencia de 27 de octubre de 2011, declaraba que no debían tomarse en consideración los objetivos perseguidos por la persona que accedía o se mantenía en el sistema, por cuanto la voluntad del titular del derecho a excluirlo sólo conecta con el dato objetivo de la estancia física del agente en el citado sistema, lo que significa que la voluntad debe ser verificada sólo con referencia al resultado inmediato de la conducta puesta en marcha, no a los sucesivos hechos[657].

---

655 COLÁS TURÉGANO, A., "Nuevas conductas delictivas ...", *cit*., nota 168, p. 678.

656 PECORELLA, C., "El acceso abusivo a los sistemas ...", *cit*., nota 434, p. 78.

657 Según dispone la Sentencia del Tribunal de Casación italiano, Sección Conjunta, de 27 de octubre de 2011, FJ 4º: "*A fronte del contrastante quadro interpretativo dianzi delineato, queste Sezioni Unite ritengono che la questione di diritto controversa non debba essere*

## *5. FORMAS DE APARICIÓN.*

Una vez expuesto el objeto material del tipo básico y los elementos delimitadores del *hacking*, en este apartado no se intentan analizar todas las formas posibles de aparición del delito de *hacking*. Únicamente se trata de repasar los supuestos con especial incidencia en el tipo del artículo 197 *bis* 1 CP. Algunos de ellos ya se han apuntado en los anteriores subepígrafes con ocasión del estudio del objeto material del delito y el elemento de "*estar debidamente autorizado*", con referencia a los sujetos que pueden autorizar (*vid.* Subepígrafe 2.2.3); o en los elementos delimitadores de facilitar el *hacking* en el artículo 197 *bis* 1 y en el artículo 197 *ter* CP, de las conductas relativas a facilitar estos comportamientos, con referencia al

---

*riguardata sotto il profilo delle finalità perseguite da colui che accede o si mantiene nel sistema, in quanto la volontà del titolare del diritto di escluderlo si connette soltanto al dato oggettivo della permanenza (per così dire "fisica") dell'agente in esso. Ciò significa che la volontà contraria dell'avente diritto deve essere verificata solo con riferimento al risultato immediato della condotta posta in essere, non già ai fatti successivi. Rilevante deve ritenersi, perciò, il profilo oggettivo dell'accesso e del trattenimento nel sistema informatico da parte di un soggetto che sostanzialmente non può ritenersi autorizzato ad accedervi ed a permanervi sia allorquando violi i limiti risultanti dal complesso delle prescrizioni impartite dal titolare del sistema (nozione specificata, da parte della dottrina, con riferimento alla violazione delle prescrizioni contenute in disposizioni organizzative interne, in prassi aziendali o in clausole di contratti individuali di lavoro) sia allorquando ponga in essere operazioni di natura ontologicamente diversa da quelle di cui egli è incaricato ed in relazione alle quali l'accesso era a lui consentito".* Sentencia disponible en http://www.penale.it/page.asp?IDPag=1021, consultado el 29 de octubre de 2016.

acto preparatorio punible que requiere su delimitación de los actos previos a la ejecución (*vid.* Subepígrafe 2.2.4 y 3.5); o en su consideración como delito de resultado, con la posibilidad de tentativa (*vid.* Capítulo III.5).

Por ello, en los siguientes apartados estudiaremos la autoría y participación, el *iter criminis*, las formas imperfectas de ejecución y las relaciones concursales en general, concluyendo con la toma de posición sobre estos puntos.

### *5.1 Autoría y participacion.*

La autoría y participación en el delito de *hacking* ya han sido parcialmente tratadas con ocasión del elemento relativo a la "*debida autorización*". Al respecto, el delito puede ser cometido por las personas físicas, sin perjuicio de la responsabilidad de las personas jurídicas según se expondrá en el Capítulo VI de este trabajo.

El presente punto se dedica a analizar estos elementos en torno al delito de *hacking* en el CP, en cuyo artículo 27 tras la reforma de la LO 1/2015 se establece que "*Son responsables criminalmente de los delitos los autores y los cómplices"*.

En este sentido, para WELZEL, en lo que se ha denominado teoría del dominio del hecho referida a la autoría y participación, la autoría presentaba una serie de exigencias: los requisitos personales,

que comprendían objetivamente las especiales posiciones de deber del autor y subjetivamente las especiales intenciones y tendencias, y los requisitos típicos, es decir, el dominio final, al entender como autor el dueño y señor del hecho, en la medida en que realiza su decisión de voluntad con sentido. La coautoría es igualmente autoría, pero presenta la especialidad de que el dominio del hecho delictivo único no corresponde a un solo sujeto sino conjuntamente a varios.

Frente a esta idea de autor inmediato, se encuentra la autoría mediata, considerando que en el autor mediato, o bien no concurrirían los requisitos personales del autor en el tercero utilizado para realizar el delito, o bien el tercero no tendría el dominio final del hecho.

Por último, la participación sería considerada como la contribución en el hecho ajeno, "*la preparación de acciones de apoyo sin participación en la decisión del hecho y en el dominio del hecho final*"[658].

Tal y como resume LUZÓN CUESTA[659], la citada teoría es una de las que combina elementos objetivos y subjetivos, acogiendo la figura de la autoría mediata, sin embargo no resuelve el problema de la autoría en los delitos imprudentes, cuestión que no afecta al delito del artículo 197 *bis* 1 CP, tal y como se expondrá en el presente epígrafe.

---

658 WELZEL, H., *Estudios de Derecho penal ...*, *cit*., nota 340, pp. 88, 89, 96 y 101.

659 LUZÓN CUESTA, J. M., *Compendio de Derecho Penal ...*, *cit*., nota 12, p. 190.

En esta línea y dentro de las distintas corrientes de la teoría del dominio del hecho, destaca la teoría de la determinación objetiva y positiva del hecho, que como señala GÓRRIZ ROYO, se caracteriza por seguir la postura del dominio del hecho pero dejando a un lado el elemento subjetivo. En concreto, incidiendo en el "dominio objetivo", basado en la condición de la realización de acciones típicas, que constituiría el presupuesto objetivo y formal[660]. Así, DÍAZ Y GARCÍA CONLLEDO concluye que autor es "*quien reuniendo los elementos personales o especiales de la autoría exigidos por algunos tipos, y cumpliendo el resto de los elementos del tipo, solo e inmediatamente (autor inmediato individual, concurran o no otros intervinientes), a través de otro al que utiliza como instrumento (autor mediato), o mediante la actuación conjunta con otros (coautor), domina el hecho, es decir determina objetiva y positivamente el curso del suceso*"[661].

Por su parte, entre la doctrina española mayoritaria se sigue la corriente denominada objetivo-formal, que se caracterizaría porque lo decisivo es la realización de un acto ejecutivo típico, relegando a considerar partícipe al sujeto que lleva a cabo otras contribuciones.

Desde los puntos de vista expuestos se van a analizar autoría y participación en relación al *hacking* en el presente punto.

---

660 GÓRRIZ ROYO, ELENA Mª, *El concepto de autor en el Derecho penal*, ed. Tirant Lo Blanch, Valencia, 2008, p. 430.

661 DÍAZ Y GARCÍA CONLLEDO, M., *La autoría en Derecho penal*, ed. PPU, Barcelona, 1991, p. 691.

Con estas premisas, sin ánimo de realizar un análisis de las teorías propias de la parte general del Derecho penal, por no ser este el lugar para tan profundo debate, podemos decir en línea con la última teoría y siguiendo a QUINTERO OLIVARES que autor del delito "*es aquel cuyo comportamiento puede ser directamente subsumido en el tipo legal*"[662], y para determinarlo, como dicen ORTS BERENGUER y GONZÁLEZ CUSSAC, deberemos preguntarnos "*quién realizó la acción típica*"[663].

Una vez expuestas estas ideas sobre la autoría y la participación, a continuación se analiza su incidencia en el delito de intrusismo informático.

*5.1.1 Autoría.*

Conforme a lo anteriormente citado y según resulta del artículo 197 *bis* 1 CP, será autor del delito de *hacking* "*El que por cualquier medio o procedimiento, vulnerando las medidas de seguridad establecidas para impedirlo, y sin estar debidamente autorizado, acceda o facilite a otro el acceso al conjunto o una parte de un sistema de información o se mantenga en él en contra de la voluntad de quien tenga el legítimo derecho a excluirlo*". En concreto, de

662 QUINTERO OLIVARES, G., con la colaboración de MORALES PRATS, F., *Parte general ...*, cit., nota 464, p. 648.

663 ORTS BERENGUER, E. y GONZÁLEZ CUSSAC, J. L., *Compendio de Derecho penal ...,cit.,* nota 465, p. 305.

conformidad con el artículo 28 CP, lo serán "*quienes realizan el hecho por sí solos, conjuntamente o por medio de otro del que se sirven como instrumento. También serán considerados autores: a) Los que inducen directamente a otro u otros a ejecutarlo. b) Los que cooperan a su ejecución con un acto sin el cual no se habría efectuado"*, de donde resultan tres formas de autoría: la inmediata, la conjunta y la mediata.

Respecto a la autoría inmediata, tiene lugar como indica QUINTERO OLIVARES cuando el autor realiza por sí mismo el delito[664]. Ya se ha hecho referencia a la conducta típica en el epígrafe 2 de este Capítulo y cada una de las circunstancias que deben concurrir en el autor del intrusismo informático, presentando mayores dificultades los otros dos supuestos.

Así, por lo que respecta a los casos de coautoría, conviene indicar en este punto que las conductas aquí estudiadas no deben confundirse con las referidas en el tipo agravado del artículo 197 *quater* CP, referido al *hacking* cometido en el seno de una organización o grupo criminal y al que se dedica el Capítulo siguiente de este trabajo.

Efectivamente, sin perjuicio de un mayor desarrollo allí, VELASCO NUÑEZ[665] describe una serie de caracteres o requisitos de

---

664 QUINTERO OLIVARES, G., con la colaboración de MORALES PRATS, F., *Parte general ...*, *cit*., nota 464, p. 648.

665 VELASCO NUÑEZ, E., "Delitos informáticos realizados en actuación organizada", en *Diario La Ley*, nº 7743, de 24 de noviembre de 2011, pp. 4 y

carácter nuclear en la agravante de pertenencia a organización/grupo/asociación en los delitos informáticos conforme a la jurisprudencia anterior a la LO 5/2010: (i) la necesidad de una pluralidad de personas coordinadas entre sí, se conozcan personalmente o no, habiendo decidido el legislador que sean más de dos personas (artículos 570 *bis* y 570 *ter* CP); y (ii) la agravante exige "pertenencia", lo cual supone excluir la colaboración accidental u ocasional, existiendo cierta vocación de continuidad, que se matiza en una "*mínima permanencia para superar la mera codelincuencia*".

No obstante, siguiendo a CEREZO MIR[666], para que exista coautoría será preciso que varias personas tengan un acuerdo de voluntades para la ejecución del hecho, perteneciendo el dominio del hecho conjuntamente a todos ellos conforme a la teoría de WELZEL expuesta más arriba, realizando cada una de ellas algún elemento del tipo, supuesto distinto a la codelincuencia, donde en la comisión del delito concurren varios delincuentes, pero es posible que uno sólo de ellos sea el autor y los demás partícipes.

Así, siguiendo el criterio jurisprudencial reflejado, entre otras, en la STS de 10 de noviembre de 2005[667], "*como, precisa la STS 590/2004 de 6.5 (RJ 2004, 5018), «se diferencia la coautoria de la*

---

5.

666 CEREZO MIR, J., *Derecho Penal. Parte General-lecciones*, ed. UNED, Madrid, 2000, p. 193.

667 STS, Sala Segunda, de 10 de noviembre de 2005, nº 1315/2005, Pte. Excmo. Sr. D. Juan Ramón Berdugo y Gómez de la Torre, FJ 3º (RJ 2006\3099).

*cooperación o de la participación, en el carácter o no, subordinado del participe a la acción del autor. Será coautor quien dirija su acción a la realización del tipo con dominio de la acción, que será funcional si existe la división de funciones entre los intervinientes, pero todas con ese dominio de la acción característico de la autoria», y se concreta que existe cooperación necesaria cuando se colabora con el ejecutor directo aportando una conducta sin la cual el delito no se habría cometido (teoría de la «condictio sine qua non»), cuando se colabora mediante la aportación de algo que no es fácil de obtener de otro modo (teoría de los bienes escasos) o cuando el que colabora puede impedir la comisión del delito, retirando su concurso (teoría del dominio del hecho), (STS 1159/2004 de 28.10 [RJ 2004, 7694])".*

De tal forma que en el *hacking*, para que exista coautoría será preciso que el acceso o el mantenimiento se produzca de forma concertada entre varios sujetos, interviniendo cada uno de ellos en su ejecución como autores, todos ellos con un dominio del hecho. Podría ser el caso del ataque simultáneo a un sistema informático convenido entre varios *hackers*, sobrepasando todos y cada uno de ellos las medidas de seguridad establecidas por su titular para proteger el sistema informático, accediendo al sistema gracias a los ataques de los otros y sin los cuales a su vez no podrían haber accedido, o la permanencia en el sistema al que han accedido de forma autorizada varios sujetos una vez retirada la autorización del titular que no se apercibe de ello porque ninguno de esos sujetos lo ha abandonado.

En cuanto a la autoría mediata, como indica DÍAZ Y GARCÍA CONLLEDO, el autor domina el hecho a través de otro al que utiliza como instrumento[668]. Esta otra persona, tal y como señala QUINTERO OLIVARES, "*actúa inconsciente de la transcendencia penal de lo que hace*"[669], de tal manera que siguiendo a GÓRRIZ ROYO, podemos decir que "ejecuta" desde el instante que comienza a actuar sobre el instrumento y éste empieza poner en marcha el tipo y, por tanto, al instrumentalizar a otro inicia la ejecución y en ese momento la conducta constituiría tentativa[670]. Como dice el ATS de 14 de mayo de 2009[671], "*la autoría mediata prevista en el art. 28 CP (quienes realizan el hecho por medio de otro) requiere, al menos en los supuestos fuera de discusión, que el instrumento sea incapaz de culpabilidad, obre con error (de tipo o de prohibición) o bajo coacción. Sólo estas circunstancias, en principio, pueden desplazar el dominio del hecho al que actúa por detrás".*

Cabe pensar por tanto en el dominio del hecho llevado a cabo mediante coacción, por violencia o amenazas sobre un sujeto para que lleve a cabo el acceso ilícito o la permanencia en el sistema

---

668 DÍAZ Y GARCÍA CONLLEDO, M., *La autoría ...*, *cit*., nota 661, p. 691.

669 QUINTERO OLIVARES, G., con la colaboración de MORALES PRATS, F., *Parte general ...*, *cit*., nota 464, p. 649.

670 GÓRRIZ ROYO, ELENA Mª, *El concepto de autor ...*, *cit*., nota 660, p. 447.

671 ATS, Sala Segunda, de 14 de mayo de 2009, nº 1114/2009, Pte. Excmo. Sr. D. Adolfo Prego de Oliver y Tolivar, FJ 2º (JUR 2009\267915), que transcribe el criterio de la STS, Sala Segunda, de 5 de febrero de 2008, nº 44/2008, recurso 1208/2007, Pte. Excmo. Sr. D. Enrique Bacigalupo Zapater, FJ 2º (RJ 2008\1723).

informático, o bien induciéndole a error o aprovechando la situación de error en la que se encuentra, sea error de tipo o por encontrarse en una situación de inimputabilidad como pudiera ser la anomalía o alteración psíquica que sufriese el sujeto/instrumento, situación de la que se aprovecharía el autor mediato para cometer el delito de *hacking* a través de este instrumento.

### *5.1.2 Participación.*

En cuanto a la participación, tal y como indica QUINTERO OLIVARES, constando descrita la autoría en el correspondiente tipo delictivo, se integraría por los demás casos previstos en el artículo 28.2, apartados a y b, y en el artículo 29 CP, que establece que "*Son cómplices los que, no hallándose comprendidos en el artículo anterior, cooperan a la ejecución del hecho con actos anteriores o simultáneos"*. Dicho en otras palabras, la participación en nuestro Código estaría integrada por la inducción, la complicidad necesaria y la no necesaria[672], con independencia de que, como dice GORRIZ ROYO, formal o legalmente se les considere autores[673].

Siguiendo a ORTS BERENGUER y GONZÁLEZ CUSSAC, los tres supuestos son actos de participación en sentido material, es

---

672 QUINTERO OLIVARES, G., con la colaboración de MORALES PRATS, F., *Parte general ...*, *cit*., nota 464, p. 657.

673 GÓRRIZ ROYO, ELENA Mª, *El concepto de autor ...*, *cit*., nota 660, p. 202.

decir, conductas accesorias. Sin embargo, por razones político-criminales, para los inductores y los cooperadores necesarios está prevista igual pena que para los autores materiales, por considerar que merecen más castigo que la complicidad no necesaria al contribuir con especial significación y trascendencia al hecho principal[674].

Por lo que respecta a los supuestos de inducción, equiparada formalmente en el artículo 28.a) CP a la autoría, la STS de 16 de marzo de 2015[675] ha establecido que: "*Según la doctrina, inductor es el que hace nacer en otro la voluntad de cometer un hecho delictivo, al ejercer un influjo psíquico sobre otra persona, que va a ser quien finalmente ejecute el hecho de manera responsable. Por su parte, la jurisprudencia de esta Sala tiene establecido, siguiendo asentados criterios doctrinales, que la inducción constituye materialmente una forma de participación de singular relevancia que tiene como sustento el influjo psíquico, logrado de diversas formas posibles, que el inductor despliega sobre otras personas (autores materiales) al objeto de que ejecuten un delito concreto y en relación también con una víctima concreta, lo que la distingue de la provocación del artículo 18 C. Penal (SSTS 421/2003, de 10-4 (RJ 2003, 3990); 503/2008, de 17-7 (RJ 2008, 5159); y 1357/2009, de 30-12 (RJ 2010, 2986))".* De tal forma que en el *hacking*, podría ser el supuesto del sujeto que influye en otro para que lleve a cabo el acceso ilícito o el mantenimiento en

674 ORTS BERENGUER, E. y GONZÁLEZ CUSSAC, J. L., *Compendio de Derecho penal ..., cit.,* nota 465, p. 315.

675 STS, Sala Segunda, de 16 de marzo de 2015, nº 155/2015, recurso 1589/2014, Pte. Excmo. Sr. D. Alberto Jorge Barreiro, FJ 2º (RJ 2015\1142).

un sistema de información, siempre y cuando el sujeto que lo ejecuta no estuviese ya decidido a cometer el delito antes[676], y siendo necesaria la efectiva ejecución, puesto que en caso contrario estaríamos en el supuesto de la proposición previsto en el artículo 17.2 CP[677], que al no tener expresa previsión en los delitos de *hacking*, determinaría la impunidad de la proposición conforme al artículo 17.3 CP.

Por otra parte, el legislador equipara al provocador con el inductor cuando el delito llega a ejecutarse, de tal manera que en el supuesto de que un sujeto incitase directamente *"por medio de la imprenta, la radiodifusión o cualquier otro medio de eficacia semejante, que facilite la publicidad, o ante una concurrencia de personas, a la perpetración de un delito"* de *hacking*, sería castigado sólo si la provocación de este delito estuviese expresamente tipificada

---

676 Así, la STS, Sala Segunda, de 14 de septiembre de 1989, Pte. Excmo. Sr. D. Francisco Soto Nieto, FJ 5º, (RJ 1989\6644) establecía que "*El inducido no ha de haber resuelto antelativamente la ejecución del hecho delictual sino que ello ha de ser consecuencia de la excitación influenciante del inductor, sin que ello signifique que previamente aquél haya de ser indiferente al hecho, o que no pueda apreciarse algún otro factor confluyente y adherido, siempre de estimación secundaria, en la determinación delictiva del agente. La inducción implica que la persona influida o instigada, además de adoptar la resolución ejecutiva del hecho antijurídico, entre en la fase realizadora del mismo, cualquiera que sea el grado alcanzado en ella. Doctrina, la expuesta que tiene su reflejo en Sentencias de esta Sala de 12 de abril de 1986 ( RJ 1986\1964) y 8 de febrero de 1988 ( RJ 1988\911)".*

677 En este sentido ha concluido, entre otras, la STS, Sala Segunda, de 29 de noviembre de 2002, nº 1994/2002, recurso 1621/2001, Pte. Excmo. Sr. D. José Ramón Soriano Soriano, FJ 2º (RJ 2002\10874).

(artículo 18 CP), por lo que en principio la conducta del provocador no estaría castigada al no existir esta tipificación. No obstante, tal y como establece el mismo precepto, "*Si a la provocación hubiese seguido la perpetración del delito, se castigará como inducción"*.

En cuanto a la cooperación necesaria, podemos seguir el criterio de la STS de 4 de febrero de 2015[678], por cuanto en su FJ 3º aglutina las teorías más relevantes en torno a su distinción respecto a la coautoría, con cita de numerosa jurisprudencia, y caracteriza la cooperación necesaria porque no existe el dominio de la acción propio de la coautoría, donde el coautor dirige su acción a la realización del tipo con dominio de la acción, mientras que el cooperador necesario en estos delitos será quien colabore en el acceso al sistema informático o en el mantenimiento no autorizado con una conducta sin la cual no se podría haber accedido o permanecido dentro de él (teoría de la *conditio sine qua non*, por ejemplo abriendo la puerta blindada

[678] STS, Sala Segunda, de 4 de febrero de 2015, nº 23/2015, recurso 10144/2014, Pte. Excmo. Sr. D. Juan Ramón Berdugo y Gómez de la Torre (RJ 2015\2792), FJ 3º: "*se diferencia la coautoría de la cooperación o de la participación, en el carácter o no, subordinado del participe a la acción del autor. Será coautor quien dirija su acción a la realización del tipo con dominio en la acción, que será funcional si existe la división de funciones entre los intervinientes, pero todas con ese dominio de la acción característico de la autoría", y existe cooperación necesaria cuando se colabora con el ejecutor directo aportando una conducta sin la cual el delito no se habría cometido (teoría de la "condictio sine qua non"), cuando se colabora mediante la aportación de algo que no es fácil de obtener de otro modo (teoría de los bienes escasos) o cuando el que colabora puede impedir la comisión del delito, retirando su concurso (teoría del dominio del hecho)".*

de la habitación donde se encuentra el ordenador al que se pretende acceder o distrayendo al titular del sistema para que otro sujeto permanezca en él), aportando algo que no es fácil de obtener de otro modo (teoría de los bienes escasos, por ejemplo aportando una copia de la llave del almacén donde se encuentra el sistema informático al que se va a acceder, o accediendo con las claves de acceso al sistema informático para que el sujeto que ya había accedido con autorización previamente pueda mantenerse en él de forma no autorizada), o cuando el que colabora puede impedir la comisión del delito retirando su concurso (teoría del dominio del hecho, por ejemplo el que facilita el cableado ethernet para poder acceder al sistema informático y puede retirar en cualquier momento el cable impidiendo la comisión del delito).

Cabe pensar también en el caso del guardia de seguridad que permite a otra persona el acceso físico a una habitación de acceso restringido donde se encuentra el sistema informático de una empresa, de tal manera que sin su colaboración no podría haber accedido o, dando un simple aviso, podría impedir el acceso ilícito o la permanencia en el sistema, y si lo hace concurriendo las circunstancias de los artículos 570 *bis* o 570 *ter* CP, concurrirá el tipo agravado del artículo 197 *quater*, que veremos en el siguiente Capítulo de este trabajo.

No obstante lo expuesto, tras la reforma del artículo 197 *bis* 1 CP por la LO 1/2015, la distinción práctica entre la autoría y la cooperación necesaria en el delito de acceso ilícito al sistema

informático se difuminará en la medida en que conforme al citado artículo serán autores tanto el que "*acceda*" como el que "*facilite a otro el acceso*", lo que supone en estos casos elevar a la categoría de autoría las conductas de cooperación.

Se plantea aquí la duda teórica de cuándo nos encontramos en el caso de la cooperación necesaria o la complicidad no necesaria del artículo 29 CP, en relación con las conductas de *hacking*.

En este punto, en principio podríamos considerar el criterio jurisprudencial reflejado en la citada STS de 4 de febrero de 2015 por la distinción que hace entre estas conductas y las de coautoría y cooperación necesaria, con cita de numerosa jurisprudencia, para definir los rasgos de la complicidad no necesaria, que entraría en el ámbito del artículo 29 CP a efectos de una hipotética aplicación en relación con el artículo 197 *bis* CP. Así, según resulta de esta STS[679],

[679] Según el FJ 3 de la citada STS de 4 de febrero de 2015, "*lo que distingue al cooperador necesario del cómplice no es el dominio del hecho, que ni uno ni otro tienen. Lo decisivo a este respecto es la importancia de la aportación en la ejecución del plan del autor o autores" (...) para que exista complicidad han de concurrir dos elementos: uno objetivo, consistente en la realización de unos actos relacionados con los ejecutados por el autor del hecho delictivo, que reúnan los caracteres ya expuestos, de mera accesoriedad o periféricos; y otro subjetivo, consistente en el necesario conocimiento del propósito criminal del autor y en la voluntad de contribuir con sus hechos de un modo consciente y eficaz a la realización de aquél, (...). En definitiva, el cómplice es un auxiliar del autor, que contribuye a la producción del fenómeno delictivo a través del empleo anterior o simultáneo de medios conducentes a la realización del proyecto que a ambos les anima, participando del común propósito mediante su colaboración voluntaria concretada en actos secundarios, no necesarios para el desarrollo del «iter criminis».*

ese cómplice del delito de acceso ilícito a un sistema informático no tendría dominio del hecho, pero realizaría actos accesorios o periféricos, con conocimiento del propósito criminal del autor y voluntad de contribuir en ese acceso.

Con estas premisas, resulta prácticamente muy difícil pensar en algún supuesto de complicidad no necesaria en el delito del artículo 197 *bis* 1 CP, por cuanto tras la citada reforma de la LO 1/2015 el legislador ha equiparado las conductas entre el que "*acceda*" y el que "*facilite a otro el acceso*", produciéndose una criticable ampliación de los supuestos de autoría[680] a los casos que, conforme a la doctrina y jurisprudencia expuesta, tendrían la consideración de participación.

Precisamente, de acuerdo con el criterio que se ha expuesto en el anterior epígrafe 2, con ocasión de la diferencia entre las conductas de facilitar el acceso del artículo 197 *bis* y las de facilitar el acceso por alguno de los medios del artículo 197 *ter* CP, podríamos reducir los casos de complicidad no necesaria de forma residual a las conductas de facilitar el acceso que no estén previstas en esos dos artículos. Así pues, esa complicidad se limitaría a los casos en los que el sujeto ayuda al acceso al sistema informático siempre que no lo hiciera facilitando los instrumentos del artículo 197 *ter* CP, excluyendo así la aplicación de este precepto como autor y, además, el acceso no tuviese éxito, eludiendo de esta forma la autoría del artículo 197 *bis* 1 CP, que como hemos visto queda reducido a los supuestos de facilitar el

[680] En este sentido, COLÁS TURÉGANO, A., "Nuevas conductas delictivas ...", *cit*., nota 168, p. 676.

acceso cuando éste no llega a producirse para así distinguirlo de las conductas del artículo 197 *ter* CP.

En el caso de las conductas de mantenimiento no autorizado en el sistema, se deberían relizar actos accesorios o periféricos, con conocimiento del propósito criminal del autor y voluntad de contribuir a esa permanencia por algún medio no encuadrable en el artículo 197 *ter* CP.

*5.2 Iter Criminis.*

Tal y como se ha apuntado en el Capítulo III, el delito de *hacking* se configura como un delito de peligro concreto para la seguridad del sistema informático al que se accede o en el que se permanece, sin perjuicio de la tutela anticipada de otros bienes jurídicos que pudieran verse afectados una vez se produjera el acceso o el mantenimiento en el sistema ya que, empleando la terminología de HURTADO ADRIÁN, se adelantan las barreras de protección en relación a eventuales ataques contra bienes jurídicos individuales[681], y esa barrera se anticipa más aun tras la reforma de 2015, por cuanto la conducta ya no se refiere al acceso a datos o programas a los que se aludía en el anterior artículo 197.3 CP tras la reforma de la LO 5/2010, sino al conjunto o una parte de un sistema de información.

[681] HURTADO ADRIÁN, A., "Accesos informáticos ilícitos ...", *cit*., nota 145, p. 127.

Por otra parte, siguiendo a ORTS BERENGUER y GONZÁLEZ CUSSAC, tal y como hemos visto en el Capítulo anterior, si son delitos de resultado aquellos que requieren un resultado, es decir, que se produzca una consecuencia que difiera de la acción, de la manifestación de la voluntad, mostrándose separada en tiempo y espacio[682], exigido en el delito de *hacking* como resultado el acceso al sistema de información o su permanencia, con riesgo para su seguridad, nos encontramos también ante un delito de resultado.

Conforme al planteamiento de VON LIST[683], toda acción criminal es forma de ejecución interna y externa, por lo que como señalan ORTS BERENGUER y GONZÁLEZ CUSSAC en la comisión del delito pueden distinguirse dos fases: la interna, que comprendería la ideación, deliberación y resolución; y la externa, que abarcaría la realización[684], lo que resulta igualmente trasladable al delito que nos ocupa. Sin ánimo de entrar ahora en la fase interna de este delito, por afectar al campo interno de la conciencia y, por tanto, resultar irrelevante jurídicamente, conviene delimitar en la medida de lo posible las fases del delito atendido el planteamiento del legislador tras la reforma de la LO 1/2015.

---

682 ORTS BERENGUER, E. y GONZÁLEZ CUSSAC, J. L., *Compendio de Derecho penal ...*, *cit*., nota 465, p. 244.

683 VON LISZT, F., *Tratado de Derecho penal ...*, *cit*., nota 247, p. 363.

684 ORTS BERENGUER, E. y GONZÁLEZ CUSSAC, J. L., *Compendio de Derecho penal ...*, *cit*., nota 465, p. 289.

En la fase externa encontraríamos, siguiendo a QUINTERO OLIVARES, los actos preparatorios, la tentativa y la consumación[685], razón por la cual presenta especial interés determinar el inicio de la fase ejecutiva a efectos de su punición o no.

### *5.2.1 Actos preparatorios.*

Los actos preparatorios se configuran según QUINTERO OLIVARES como primeros actos externos que pueden determinar consecuencias juridico-penales, siendo su número incalculable, razón por la cual, conforme al principio de legalidad, el Código opta por describir los actos preparatorios punibles. En concreto, la conspiración, la proposición y la provocación para delinquir[686]. Así pues, cabe excluir de la fase de ejecución las resoluciones manifestadas, también entendidas como actos de manifestación de voluntad[687], y que sólo son castigadas en los casos expresamente previstos, tal y como establecen los artículos 17.3 (para la conspiración y la proposición) y 18.2 (para la provocación) CP. En el supuesto del *hacking* no están expresamente tipificadas las citadas resoluciones, por lo que la conspiración, proposición y provocación

685 QUINTERO OLIVARES, G., con la colaboración de MORALES PRATS, F., *Parte general …*, *cit*., nota 464, p. 607.

686 *Ibíd.*, p. 607.

687 Así, LUZÓN CUESTA, J. M., *Compendio de Derecho Penal …*, *cit*., nota 12, p. 179.

para cometer el delito no serían castigadas. No obstante, siguiendo la regulación de la provocación en el artículo 18 CP, en el supuesto de que un sujeto incitase directamente a otro u otros "*por medio de la imprenta, la radiodifusión o cualquier otro medio de eficacia semejante, que facilite la publicidad, o ante una concurrencia de personas, a la perpetración de un delito"* de *hacking*, aunque no está expresamente castigada la provocación para estos delitos por lo que en principio no sería punible conforme al artículo 18.2 CP, si la infracción llegase a ejecutarse entonces el sujeto provocador será castigado como inductor, tal y como concluye el mismo precepto ("*Si a la provocación hubiese seguido la perpetración del delito, se castigará como inducción"*).

Por otra parte, el citado régimen de la provocación determina que la apología para llevar a cabo estos delitos tampoco se castigue en nuestro Código Penal. Esta figura se define en el artículo 18.1 CP como "*la exposición, ante una concurrencia de personas o por cualquier medio de difusión, de ideas o doctrinas que ensalcen el crimen o enaltezcan a su autor*" del delito de intrusismo informático, según el mismo precepto, "*La apología sólo será delictiva como forma de provocación y si por su naturaleza y circunstancias constituye una incitación directa a cometer un delito*", no estando expresamente penada la provocación del acceso ilícito o permanencia no autorizada en un sistema de información, tampoco podrá serlo la apología de estos delitos salvo que se produjese la efectiva

perpetración del delito tras la incitación directa, hecho que podría reconducirse a la inducción conforme al citado artículo 18.2 CP.

### *5.2.2 Tentativa.*

Considerando el instrusismo informático un delito de resultado, como tal cabe la imperfecta ejecución según señala QUERALT JIMÉNEZ[688], por cuanto no sólo hay que llevar a cabo la intrusión en el conjunto o parte del sistema, sino que también deben vulnerarse las medidas de seguridad, concurriendo la separación espacio-temporal propia de los delitos de resultado.

Al respecto, para determinar el inicio de la realización del delito se han planteado diversas teorías, apuntándose a continuación algunas de las más relevantes, a efectos de delimitar la ejecución en el delito de *hacking*.

Así, para CARRARA la tentativa se caracterizaba por ser un principio de ejecución, un acto externo, que unívocamente llevaba al delito, pero en el caso de que el acto externo pueda conducir al delito o igualmente a un acto inofensivo estaremos ante un acto preparatorio impune. Este autor planteaba el caso del que accede a un domicilio ajeno, que será un delito de violación de domicilio, pero si lo hace entrando a mi habitación con un puñal en la mano, sería tentativa de

688 QUERALT JIMÉNEZ, J. J., *Derecho penal español ..., cit.*, nota 11, p. 340.

homicidio[689]. Esta idea, trasladada al acceso ilícito al sistema de información y atendido el paralelismo ya apuntado anteriormente entre estos delitos y los de allanamiento de morada[690], nos lleva a que, de forma paralela con el ejemplo, el que enciende su ordenador y curiosea de forma remota alrededor de un sistema informático ajeno sin acceder a él, no cometerá en principio delito alguno, pero si lo hace habiendo instalado previamente un generador de claves de acceso en su ordenador configurado para acceder ilícitamente a ese sistema ajeno y poner en peligro su seguridad, evidenciando que su conducta iba inequívocamente dirigida a cometer el delito del artículo 197 *bis* 1 CP, sería comienzo de la ejecución y por tanto tentativa de este delito.

Por su parte, con referencia a la fase de ejecución, BELING también se refería a la tentativa como "comienzo de ejecución", quedando impunes las acciones que todavía no son adecuadas, denominadas preparatorias, perteneciendo al núcleo del tipo los actos que suponen el inicio de la acción descrita en el verbo empleado en el tipo, siendo actos preparatorios los demás[691]. Esta postura plantea problemas en la práctica, pensemos en el caso del que adquiere un programa para acceder a un sistema informático de forma remota y lo

---

689 CARRARA, F., *Programa de Derecho Criminal …*, *cit*., nota 513, pp. 247 y 248.

690 *Vid., supra* Capítulo III, subepígrafe 3.5 y Capítulo IV, subepígrafe 2.2.5.

691 BELING, E. V., *Esquema de Derecho Penal. La doctrina del delito – tipo*, ed. Librería "El Foro", Buenos Aires, 2002, traducido por SOLER, S., pp. 132-139.

deja en su ordenador instalado pero, antes de utilizarlo, un tercero usuario del mismo ordenador lo ejecuta por error siendo el que comete el delito. Sin perjuicio del error de tipo que pudiera apreciarse en el tercero que ejecuta el acceso, parece difícil delimitar cuándo el primer sujeto ha comenzado la ejecución del delito que nos ocupa según esta teoría.

Por último, para MAYER eran actos de ejecución los que atacaban o ponían en peligro un bien jurídico, mientras que las acciones preparatorias dejaban el estado pacífico del bien sin alterar[692]. Conforme a esta última postura, igualmente resulta difícil delimitar los actos preparatorios del *hacking*, más aún tras la reforma de la LO 1/2015, con la que, como hemos visto, se equipara la conducta del acceso con la de facilitar el acceso, castigándose con la misma pena en el artículo 197 *bis* 1 CP. Dicho en otras palabras, no es fácil saber cuándo se ha empezado a atacar la seguridad del sistema de información.

Por tanto, la doctrina que parece más sencilla para delimitar los actos preparatorios del delito de acceso ilícito a los sistemas informáticos respecto a su ejecución es la planteada por CARRARA, sin entrar en este trabajo a analizar los matices que posteriormente surgieron en torno a ella[693], entendiendo así que cuando el sujeto realice actos que por sí mismos evidencien unívocamente la intención

---

692 MAYER, M. E., *Derecho Penal. Parte General*, ed. B de f, Buenos Aires, 2007, traducido por POLITOFFF LIFSCHITZ, S., pp. 437 y 438.

693 Así, entre otros, ANTOLISEI, F., *Manual de Derecho Penal ...*, *cit*., nota 442, p. 342.

de acceder o mantenerse ilícitamente en el sistema o facilitar el acceso, estaremos en la fase de ejecución del delito tipificado en el artículo 197 *bis* 1 CP, mientras que cuando el acto que se realice pueda llevar a la ejecución del delito o a cualquier otro acto no ofensivo, será un acto preparatorio impune, como sucedería, por ejemplo, en el caso del sujeto que sin autorización comprueba las medidas de seguridad de un sistema informático ajeno sin quebrantarlas; o elaborar un generador de claves, sin utilizarlo ni ofrecerlo, que permitiese, si se llegara a ejecutar, la generación de una clave para poder acceder al sistema informático propio en el caso de bloqueo accidental pero que igualmente fuera válido para poder acceder ilícitamente a un sistema ajeno.

Por ello, con la nueva redacción del precepto se aprecia un *iter criminis* con rasgos expansivos, donde se anticipa la tutela de la seguridad de los sistemas informáticos incluso al momento de facilitar la conducta, bien aportando alguno de los instrumentos que se citan en el artículo 197 *ter* CP, o bien facilitándola de cualquier otra forma conforme al artículo 197 *bis* 1 CP, siempre que como ya se ha apuntado, en este último caso se produzca un efectivo acceso al sistema, por coherencia penológica con la conducta de acceso. De esta forma, en estos preceptos se produce un castigo expreso de lo que son actos preparatorios del delito, alterando la regla general de la impunidad de los actos preparatorios en el Código Penal y que, como indica JORGE BARREIRO[694] con ocasión del artículo 197 *ter* CP,

[694] JORGE BARREIRO, A., "Delitos contra la intimidad ...", *cit*., nota 519,

están presuntamente preordenados a la comisión de los delitos del artículo 197 *bis* CP.

Analizando propiamente la tentativa del delito que nos ocupa, entendida con MEZGER como comienzo de la ejecución pero quedando ésta en un torso[695], o como fase externa del delito y principio de la ejecución del delito[696], el legislador español establece la definición legal en el artículo 16 CP: "*Hay tentativa cuando el sujeto da principio a la ejecución del delito directamente por hechos exteriores, practicando todos o parte de los actos que objetivamente deberían producir el resultado, y sin embargo éste no se produce por causas independientes de la voluntad del autor*".

La ejecución se realiza para conseguir el resultado, pudiendo tener lugar su producción, mientras que si no se produce, es decir, si no tiene lugar el acceso ilícito, puede serlo, siguiendo el planteamiento de QUINTERO OLIVARES[697] (i) porque existe una interrupción involuntaria, tradicionalmente considerada tentativa, o bien porque se ejecuten todos los actos para el acceso pero sin lograrlo de forma involuntaria, anteriormente denominada frustración, que el legislador ahora agrupa en el artículo 16 CP como tentativa; (ii) porque no se

---

p. 1062.

695 MEZGER, E., *Tratado de Derecho penal*, Tomo II, ed. Revista de Derecho privado, segunda edición, Madrid, 1933, traducido por RODRÍGUEZ MUÑOZ, J.A., p. 195.

696 Definido así, entre otros, por CEREZO MIR, J., *Derecho Penal ...*, *cit*., nota 666, p. 164.

697 QUINTERO OLIVARES, G., con la colaboración de MORALES PRATS, F., *Parte general ...*, *cit*., nota 464, pp. 621-628.

produzca el acceso por una interrupción voluntaria en la ejecución decidida por el propio autor, esto es, por desistimiento, o bien porque exista una ejecución completa sin éxito voluntario, llamada arrepentimiento activo; o (iii) porque el proceso iniciado para el acceso o el mantenimiento no se adecúa al tipo, razón por la cual no se puede realizar, dando lugar a la tentativa inidónea, o bien porque aun siendo adecuados los actos realizados, no se puede cometer el delito por inexistencia de objeto:

(i) En primer lugar, por lo que respecta a la frustración y tentativa del acceso ilícito, que el artículo 16.1 CP agrupa bajo tentativa, equivaliendo respectivamente a tentativa acabada e inacabada, tiene especial relevancia a los efectos de la aplicación de la pena inferior en uno o dos grados a la señalada por el artículo 197 *bis* 1 CP, tal y como ordena el artículo 62 CP[698].

Sin ánimo de analizar aquí las distintas teorías en torno a esas dos modalidades por no ser este el lugar de su estudio, vamos a seguir el criterio jurisprudencial, es decir, el de la teoría mixta que expone, entre otras, la STS de 8 de octubre de 2013[699], donde se atiende al

---

[698] El artículo 62 CP establece que "*A los autores de tentativa de delito se les impondrá la pena inferior en uno o dos grados a la señalada por la Ley para el delito consumado, en la extensión que se estime adecuada, atendiendo al peligro inherente al intento y al grado de ejecución alcanzado.*".

[699] La STS, Sala Segunda, de 8 de octubre de 2013, nº 703/2013, recurso 10263/2013, Pte. Excmo. Sr. D. Juan Ramón Berdugo y Gómez de la Torre, FJ 8º, (RJ 2014\424) "*Para determinar la distinción entre la tentativa acabada e inacabada -nos dice la STS. 817/2007 de 15.10 (RJ 2007, 6965) - se han manejado doctrinalmente dos teorías: una subjetiva, que pone el*

"*plan del autor*" y "*la objetivación de la actividad desplegada*" para así conocer "*las características internas de lo querido por el agente*" y "*llegar a determinar el grado de ejecución alcanzado por el delito*".

Así pues, siguiendo esta postura, existirá tentativa acabada del acceso ilícito al sistema informático cuando "*los actos realizados, los instrumentos utilizados y la mecánica comisiva hubieran podido producir objetivamente el resultado perseguido según el plan del autor*"[700].

Con estas premisas, podemos decir, siguiendo el ejemplo de HURTADO ADRIÁN[701], que será posible que el acceso no se produzca, porque una vez iniciado el proceso el sujeto no sea capaz de

---

*acento en el plan del autor, o sea, en el signo interno del propósito del mismo, conforme a la cual, si lo que el sujeto quería llevar a cabo era la total consumación del hecho, estaremos en presencia ya de una tentativa acabada; y otra teoría, de características objetivas, que pone el punto de vista en la secuencia de actos verificada antes de la interrupción forzada del hecho, de modo que si se han practicado todos aquellos actos que debieran dar como resultado el delito, y éste no se produce en todas sus consecuencias por causas ajenas a la voluntad del culpable, estamos en presencia de la tentativa acabada. La inacabada, sin embargo, admite aún el desistimiento voluntario del autor, con los efectos dispuestos en el art. 16.2 del Código penal. En realidad, lo correcto es seguir una teoría mixta, pues el plan del autor es necesario para distinguirlo de otros tipos delictivos y conocer las características internas de lo querido por el agente, y la objetivación de la actividad desplegada es necesaria para llegar a determinar el grado de ejecución alcanzado por el delito.".*

[700] Empleando así los términos del FJ 5º de la STS, Sala Segunda, de 2 de noviembre de 2011, nº 1125/2011, recurso 972/2011, Pte. Excmo. Sr. D. Juan Ramón Berdugo y Gómez de la Torre, (RJ 2012\1380).

[701] HURTADO ADRIÁN, A., "Accesos informáticos ilícitos ...", *cit*., nota 145, p. 126.

quebrantar las medidas de seguridad (tentativa inacabada) o porque vulneradas no se consiga acceder al sistema de información (tentativa acabada), con las consecuencias del artículo 62 del CP, y además para ello se habrán considerado los actos, instrumentos y la mecánica empleada por el sujeto para llevar a cabo el acceso y puesta en peligro del sistema, por cuanto si con estos elementos se hubiese podido producir objetivamente el resultado del acceso al sistema pretendido, estaremos ante la tentativa acabada del delito del artículo 197 *bis* 1 CP, mientras que si no se hubiese podido alcanzar el resultado, será la modalidad inacabada.

(ii) El segundo supuesto, referido a la falta de acceso al sistema informático por voluntad del autor, puede tener lugar porque decida interrumpir voluntariamente los actos de ejecución, dando lugar al desistimiento del delito, o bien porque realice una ejecución completa sin éxito voluntario, produciendo el arrepentimiento activo.

La distinción resulta trascendente a los efectos de exención de responsabilidad penal, sin perjuicio de la que pudiese concurrir por los actos ya ejecutados, de conformidad con el artículo 16 CP, apartados 2 y 3. El problema se encuentra en delimitar cuándo existe voluntariedad para interrumpir la actuación que lleva al acceso o para que no llegue a producirse ese resultado a pesar de haber ejecutado todos los actos.

Para establecer esa delimitación, aquí se sigue una vez más el criterio que ha venido fijando la jurisprudencia respecto a otros delitos, y que atiende a que "*el desistimiento, ha de ser, propio,*

*voluntario, personal y definitivo, pudiéndose destacar que cuando, el citado desistimiento, se produce porque han surgido obstáculos insuperables que impiden de modo absoluto la continuación delictiva, dicho desistimiento, se reputa involuntario e ineficaz*"[702]. De tal manera que si el sujeto que inicia el delito de *hacking*, de forma voluntaria, personal y definitiva, y sin ningún obstáculo insuperable que le impidiese acceder al sistema, decide no culminar todos los actos de ejecución, estaremos ante el desistimiento, tal y como sucedería en el ejemplo del que se conecta remotamente a otro sistema para acceder ilícitamente y ejecutados parte de los programas que permiten quebrantar las medidas de seguridad establecidas, decide voluntariamente dejar de ejecutar el que le facilitaría la clave de acceso al sistema informático ajeno. En caso contrario, siguiendo el criterio anterior de la tentativa inacabada e inacabada, si ha surgido un obstáculo insuperable para alcanzar ese resultado, impidiendo la ejecución de todos los actos, como sucedería si el último programa resulta no ser ejecutable e inesperadamente el sujeto no puede ejecutarlo para acceder, no existirá un desistimiento, sino una tentativa inacabada. El sujeto no accederá porque no puede acceder.

Pero si se han ejecutado todos los actos para el acceso, y el resultado no se produce por la decisión del sujeto que realiza ese acceso, tendrá lugar el arrepentimiento activo, lo que sucedería en el citado ejemplo del que se conecta remotamente a otro sistema para

[702] Empleando aquí los términos del Considerando 4º de la STS, Sala de lo Criminal, de 7 de junio de 1985, Pte. Excmo. Sr. D. Luis Vivas Marzal, (RJ 1985\2973).

acceder ilícitamente y ejecutados los programas que permiten quebrantar las medidas de seguridad, habiendo obtenido ilícitamente la clave de acceso a ese sistema, e introducida, mientras carga el acceso decide apagar su ordenador y, por tanto, no acceder. Por el contrario, si no ha sido el sujeto quien ha llevado la actuación para evitar que el resultado se produzca, entiendo que se producirá la tentativa acabada, lo que en el ejemplo citado, sucedería si el titular del sistema al que se pretende acceder se cerciora de que se están tratando de quebrantar la seguridad de su ordenador y decidiera cambiar las medidas de seguridad y además reforzarlas, hasta tal punto de resultar un escollo insalvable para el sujeto que pretendía acceder.

(iii) En cuanto a la tentativa inidónea y al delito imposible, como delito de peligro concreto para el sistema informático afectado, la conducta deberá ser idónea para poner en peligro la seguridad informática[703]. Esto implica que, en los supuestos en que los medios utilizados no sean idóneos para producir el acceso al sistema informático, como sucedería si se pretendiera acceder desde un *e-reader* al sistema del CNI, estaremos ante la tentativa inidónea del delito de *hacking*. Mientras que si lo que sucede es que falta el objeto, por ejemplo, un sujeto entra en un edificio para llegar hasta el habitáculo donde supuestamente se encuentra su sistema informático para una vez allí acceder al mismo, pero una vez en el lugar

[703] En este sentido, JORGE BARREIRO, A.. "Delitos contra la intimidad ...", *cit*., nota 519, p. 1065.

comprueba que el edificio no cuenta con sistema informático, tendría lugar un delito imposible.

Por último, como se ha anticipado[704], la conducta del mantenimiento se configura como una conducta omisiva trasladada al sistema informático, planteándose el problema de su consumación al requerir de una cierta permanencia temporal mínima dentro del sistema. Parece que ante la falta de claridad legislativa, la determinación del momento de consumación deberá individualizarse en cada caso, acreditando el momento hasta el cual el tercero fue autorizado a permanecer y la capacidad objetiva para lesionar el interés de la persona que tenga el legítimo derecho de excluirle poniendo en peligro la seguridad del sistema. Todos estos problemas interpretativos dificultarán la existencia de tentativa en esta modalidad.

Por lo que respecta al supuesto de facilitar las conductas de acceso, en la medida en que, como se ha expuesto[705], estos supuestos del artículo 197 *bis* 1 requieren que se produzca el efectivo acceso al sistema por el sujeto al que se le ha facilitado, si no se alcanza, la conducta será encuadrable en el marco del artículo 197 *ter*.

704 *Vid., supra* epígrafe 3.6 de este Capítulo.

705 *Vid., supra* subepígrafe 3.5 de este Capítulo.

### *5.2.3 Consumación.*

Como indica QUINTERO OLIVARES, para la consumación la ley penal no considera preciso establecer un concepto, en la medida que todas las descripciones de la parte especial del Código son de delitos consumados.

Esa consumación tiene lugar cuando se realizan todos los elementos comprendidos en la figura del delito, es decir, coincidencia total entre los hechos y el tipo del delito, de tal manera que en los delitos instantáneos se produce cuando el acto da lugar al resultado previsto y en los delitos permanentes el resultado se logra al ofender el bien jurídico, pero la consumación se prolonga en el tiempo mientras dure esa ofensa[706].

Por su parte, siguiendo a ORTS BERENGUER y GONZÁLEZ CUSSAC, en los delitos de resultado la consumación exige que además de la realización íntegra de la conducta típica, se produzca el resultado también típico[707].

De esta forma si, como hemos visto anteriormente[708], consideramos el delito de instrusismo informático como un delito instantáneo en cuanto a las conductas de acceso, y de resultado, exigirá para su consumación el efectivo acceso al sistema de información con los requisitos expuestos en el anterior epígrafe 2 de

---

706 QUINTERO OLIVARES, G., con la colaboración de MORALES PRATS, F., *Parte general ...*, *cit*., nota 464, p. 632.

707 ORTS BERENGUER, E. y GONZÁLEZ CUSSAC, J. L., *Compendio de Derecho penal ...*, *cit*., nota 465, p. 303.

708 *Vid., supra* Capítulo III, epígrafe 5.

este Capítulo, mientras que en los supuestos de facilitar las conductas de acceso será necesario que finalmente se haya producido ese acceso, por cuanto en otro caso nos encontraremos ante el supuesto del artículo 197 *ter*.

Así pues, siguiendo a JORGE BARREIRO[709], el delito quedaría consumado con el acceso en el sistema informático, por ejemplo, accediendo a la cuenta de usuario ajena en una red social, bien a su conjunto comprendiendo toda la configuración de esa cuenta, o bien a una parte de esa cuenta, como sería un grupo privado comprendido en la mencionada cuenta.

También se consumaría, en relación con la segunda de las conductas del artículo 197 *bis* 1 CP, en el caso de un acceso lícito pero cuando el sujeto se mantuviese después de que existiese una voluntad contraria a esa permanencia, manifestada por el titular del derecho de exclusión.

Estas conductas referidas al mantenimiento en el sistema después de un acceso lícito constituirán un delito permanente, en cuyo caso el estadio consumativo se prolongará en tanto se permanezca ilícitamente en el sistema de información.

[709] JORGE BARREIRO, A., "Delitos contra la intimidad ...", *cit*., nota 519, p. 1065.

### *5.3 Relaciones concursales.*

Una vez analizados el fundamento y naturaleza del delito de *hacking* como delito de peligro y resultado, su objeto y el *iter criminis*, se exponen en el presente apartado las cuestiones concursales en general, viendo en el siguiente capítulo las relaciones concursales con el delito tipificado en el artículo 197 *quater* CP.

El estudio de esta relaciones se plantea desde el punto de vista de los supuestos que se nos presentan como más comunes en concurrencia con el delito que se está estudiando.

Según se viene exponiendo, la regulación del delito de intrusismo informático en nuestro ordenamiento supone un adelantamiento de las barreras de protección de los bienes jurídicos que pueden verse afectados, en relación con los datos o programas informáticos tras la reforma de la LO 5/2010, pero con un mayor adelantamiento todavía tras la reforma de la LO 1/2015, en la medida en que ni siquiera se requiere acceder ahora a esos datos o programas.

Por tanto, son varias las situaciones concursales que nos podemos encontrar, entre ellas:

### *5.3.1 El hacking del artículo 197 bis 1 y la conducta del artículo 197 ter.*

Cabe plantear el delito de acceso al sistema de información desde un punto de vista anterior a su comisión. En concreto, en relación concursal con los actos preparatorios tipificados en el artículo 197 *ter* CP.

La peculiaridad del artículo 197 *ter*, según se ha expuesto anteriormente[710], se encuentra en que la acción se refiere a proporcionar instrumentos concretos para el acceso (un programa informático, una contraseña de ordenador, un código de acceso o datos similares a una contraseña o un código de acceso), pero precisamente esa ambigüedad en cuanto a facilitar "*datos similares*" a "*una contraseña de ordenador*" o "*un código de acceso*" puede plantear la concurrencia entre estos supuestos y los de facilitar el acceso, sin más, previsto en el artículo 197 *bis* 1.

En este caso se produciría un concurso de normas que, *a priori*, parece que se deberá resolver conforme al principio de especialidad del artículo 8 CP a favor del 197 *ter*. Esto es debido a las peculiaridades que este precepto presenta, de características más específicas que la conducta de facilitar el acceso de forma genérica prevista en el artículo 197 *bis* 1.

---

710 *Vid., supra* Capítulo IV, subepígrafe 2.2.4.

Sin embargo, en la práctica será de difícil solución, atendida la redacción del artículo 197 *ter* con alusiones a "*de cualquier otro modo, facilite a terceros*", lo que en última instancia llevará a resolver el concurso atendiendo al criterio de que efectivamente se produzca el acceso.

De esta forma, si se facilita la conducta de *hacking* y el acceso se produce, por coherencia penológica entre acceder y facilitar sería encuadrable la conducta en el artículo 197 *bis* 1 siguiendo tanto a CASTELLÓ NICÁS[711] como a COLÁS TURÉGANO[712]. Así, el concurso se resolvería conforme al principio de consunción o absorción, castigando tanto el facilitar la conducta cuando se produce el efectivo acceso como el acceso en sí, que el legislador equipara en el artículo 197 *bis* 1, mientras que si no se llega a producir el acceso, dada la especialidad de los medios en el artículo 197 *ter*, se debería resolver el concurso a favor de la aplicación de este último precepto.

En cualquier caso, como se ha indicado anteriormente, en la mayoría de los supuestos se producirá un inadecuado solapamiento de ambas figuras delictivas, de difícil delimitación, que llevará a efectos prácticos a la aplicación 197 *ter*.

Cuestión distinta será el supuesto en el cual el sujeto facilita medios para la comisión del *hacking* y a su vez también lleva a cabo el

---

711 CASTELLÓ NICÁS, N., "Delitos contra la intimidad ...", *cit*., nota 396, p. 509.

712 COLÁS TURÉGANO, A., "El delito de instrusismo informático ...", *cit*., nota 45, p. 224.

delito del artículo 197 *bis* 1. En estos casos parece más adecuado considerar la conducta como un delito continuado de acceso ilícito, que se ajustaría a la previsión y consecuencias del artículo 74.1 CP ("*... el que, en ejecución de un plan preconcebido o aprovechando idéntica ocasión, realice una pluralidad de acciones u omisiones que ofendan a uno o varios sujetos e infrinjan el mismo precepto penal o preceptos de igual o semejante naturaleza, será castigado como autor de un delito o falta continuados con la pena señalada para la infracción más grave, que se impondrá en su mitad superior, pudiendo llegar hasta la mitad inferior de la pena superior en grado*").

### *5.3.2 El hacking del artículo 197 bis 1 y el allanamiento de morada de los artículos 202.1 y 203.1.*

También hemos visto[713] que el delito de *hacking* comprende tanto la conducta de acceso remoto, sin necesidad de desplazamiento alguno, como el físico, lo cual lleva a considerar también la concurrencia entre protección de la seguridad del sistema informático y la protección del domicilio físico, es decir, el posible concurso entre el acceso ilícito al sistema informático del artículo 197 *bis* 1 y el

[713] *Vid.*, *supra* este Capítulo, subepígrafe 2.2.2.

allanamiento de morada del artículo 202.1 CP[714] o del artículo 203.1 CP[715].

En estos casos, si partimos de la modalidad medial como la "*instrumental o teleológica, la cual se da cuando un delito sea medio o necesario para cometer otro acudiendo, el legislador, para la punición de esas plúrimes conductas, primordialmente, a criterios de absorción -la pena correspondiente al delito más grave en su grado máximo- y, subsidiariamente, en tanto en cuanto esa solución sea perjudicial para el reo, a principios de acumulación matemática, esto es, sancionando los delitos separadamente"* (STS de 21 de mayo de 1990[716]), podemos concluir que el acceso físico al sistema informático, como infracción más grave, absorberá al allanamiento de morada con las consecuencias del artículo 77.3 CP[717].

---

[714] El artículo 202.1 del CP establece: "*El particular que, sin habitar en ella, entrare en morada ajena o se mantuviere en la misma contra la voluntad de su morador, será castigado con la pena de prisión de seis meses a dos años".*

[715] El artículo 203.1 del CP dispone: "*Será castigado con las penas de prisión de seis meses a un año y multa de seis a diez meses el que entrare contra la voluntad de su titular en el domicilio de una persona jurídica pública o privada, despacho profesional u oficina, o en establecimiento mercantil o local abierto al público fuera de las horas de apertura*".

[716] FJ 1º de la STS, Sala Segunda, de 21 de mayo de 1990, Pte. Excmo. Sr. D. Luis Vivas Marzal, (RJ 1990\4202).

[717] Tras la reforma de la LO 1/2015, el artículo 77.3 CP establece respecto a la modalidad medial, que "*se impondrá una pena superior a la que habría correspondido, en el caso concreto, por la infracción más grave, y que no podrá exceder de la suma de las penas concretas que hubieran sido impuestas separadamente por cada uno de los delitos. Dentro de estos límites, el juez o tribunal individualizará la pena conforme a los criterios*

La situación será diferente en el caso del acceso a un sistema informático que permita el control monitorizado del interior de una vivienda o establecimiento, por cuanto como indican ANARTE BORRALLO y DOVAL PAÍS[718], en estos casos la concurrencia entre el allanamiento de morada y el *hacking* será meramente aparente, puesto que para el allanamiento se requiere efectiva entrada (o permanencia), por lo que accediendo al sistema informático no tendría lugar el delito de allanamiento de morada. Distinta sería la situación de ese acceso al sistema informático llevado a cabo como medio necesario para allanar una vivienda o establecimiento, por ejemplo, cuando el intrusismo en el sistema se realiza para desde el monitor comprobar cuándo se puede acceder a esos espacios con éxito porque no hay vigilancia. En este caso, se produciría un concurso medial que se resolvería conforme al artículo 77.3 del CP.

### *5.3.3 El hacking del artículo 197 bis 1 y las conductas del artículo 197.2.*

Cabe también la posibilidad de que el acceso lo sea para la comisión del delito tipificado en el artículo 197.2 CP ("*Las mismas penas se impondrán al que, sin estar autorizado, se apodere, utilice o*

---

*expresados en el artículo 66. En todo caso, la pena impuesta no podrá exceder del límite de duración previsto en el artículo anterior.".*

[718] ANARTE BORRALLO, E. y DOVAL PAIS, A., "Límites de la ley penal ...", *cit*., nota 24, p. 32.

*modifique, en perjuicio de tercero, datos reservados de carácter personal o familiar de otro que se hallen registrados en ficheros o soportes informáticos, electrónicos o telemáticos, o en cualquier otro tipo de archivo o registro público o privado. Iguales penas se impondrán a quien, sin estar autorizado, acceda por cualquier medio a los mismos y a quien los altere o utilice en perjuicio del titular de los datos o de un tercero*") que tal y como recuerda MORALES PRATS[719] incorpora elementos subjetivos del injusto, a diferencia del artículo 197 *bis* 1, que no requiere una intencionalidad específica añadida al dolo. Esto supone que en el caso de que el sujeto accediese al sistema informático apoderándose de datos reservados o sin estar autorizado acceda a ellos, dará dar lugar al concurso de normas entre el delito del artículo 197 *bis* 1 CP y el del artículo 197.2 CP, quedando absorbido por éste último. De esta forma, como indicaban ANARTE BORRALLO y DOVAL PAÍS con ocasión del artículo 197.3 en su redacción dada tras la LO 5/2010, ante la identidad de bienes jurídicos o al menos de línea de ataque, se aplicaría el criterio de la consunción del delito cuyo umbral típico se ubica más lejos de la afección al bien jurídico protegido[720].

719 MORALES PRATS, F., "Título X. Delitos contra la intimidad …", *cit*., nota 369, p. 486.

720 ANARTE BORRALLO, E. y DOVAL PAIS, A., "Límites de la ley penal ...", *cit*., nota 24, p. 31.

### *5.3.4 El hacking del artículo 197 bis 1 y las conductas del artículo 264.*

El acceso abusivo va a constituir en la mayoría de los casos un paso previo a la comisión del delito de daños informáticos regulado en el artículo 264 CP[721], pasando esta conducta tras la LO 5/2010, tal y como indica MORALES GARCÍA[722], de constituir una tentativa del delito de daños cuando no se llega a causar el daño por causas independientes a la voluntad del autor, a constituir un delito consumado de *hacking*, que como hemos visto es un delito autónomo de peligro concreto que conllevaría mayores penas que la tentativa de daños, a la que absorbería.

Sin embargo, en el supuesto de que el daño pretendido sea efectivamente causado una vez realizado el acceso, se producirá el concurso ideal en su versión medial, en cuanto el acceso se configura como un medio necesario para causar el daño que, al estar consumado, absorbería al *hacking* con las consecuencias del artículo 77.3 CP.

Distinto sería el caso que plantean ANARTE BORRALLO y DOVAL PAÍS en el que una vez consumado el intrusismo, se decide

---

721 El artículo 264 CP establece en su primer apartado: "*El que por cualquier medio, sin autorización y de manera grave borrase, dañase, deteriorase, alterase, suprimiese o hiciese inaccesibles datos informáticos, programas informáticos o documentos electrónicos ajenos, cuando el resultado producido fuera grave, será castigado con la pena de prisión de seis meses a tres años".*

722 MORALES GARCÍA, O., "Delincuencia informática ...", *cit*., nota 142, p. 187.

causar daños informáticos o, al revés, cuando provocados daños informáticos, se realiza el acceso ilícito con posterioridad, en cuyo caso se produciría un concurso real[723].

### *5.3.5 El hacking del artículo 197 bis 1 y otros delitos.*

Por último, atendidas las características que se vienen exponiendo del delito de *hacking*, son numerosos los delitos que pueden venir precedidos de un previo acceso ilícito al sistema informático ajeno. Así, los casos del delito de *grooming* (artículo 183 *ter*[724]), donde siguiendo a ANARTE BORRALLO y DOVAL PAÍS[725],

---

723 ANARTE BORRALLO, E. y DOVAL PAIS, A., "Límites de la ley penal ...", *cit*., nota 24, p. 33.

724 El artículo 183 *ter* CP dispone "*1. El que a través de internet, del teléfono o de cualquier otra tecnología de la información y la comunicación contacte con un menor de dieciséis años y proponga concertar un encuentro con el mismo a fin de cometer cualquiera de los delitos descritos en los artículos 183 y 189, siempre que tal propuesta se acompañe de actos materiales encaminados al acercamiento, será castigado con la pena de uno a tres años de prisión o multa de doce a veinticuatro meses, sin perjuicio de las penas correspondientes a los delitos en su caso cometidos. Las penas se impondrán en su mitad superior cuando el acercamiento se obtenga mediante coacción, intimidación o engaño. 2. El que a través de internet, del teléfono o de cualquier otra tecnología de la información y la comunicación contacte con un menor de dieciséis años y realice actos dirigidos a embaucarle para que le facilite material pornográfico o le muestre imágenes pornográficas en las que se represente o aparezca un menor, será castigado con una pena de prisión de seis meses a dos años*".

725 ANARTE BORRALLO, E. y DOVAL PAIS, A., "Límites de la ley penal ...", *cit*., nota 24, p. 32.

podemos concluir que se produciría un concurso real de delitos, por cuanto no podría considerarse el acceso al sistema informático como un medio que fuera únicamente dirigido al contacto con el menor, sino que al menos causaría también un peligro para la intimidad y datos personales del menor. A la misma conclusión se llegaría si el acceso al sistema informático ajeno fuese para la captación de menores con finalidad exhibicionista o pornográfica, prevista en el artículo 189.1.a) CP[726].

No obstante, distinta sería la consecuencia si el acceso ilícito fuese para la comisión de un delito de estafa informática (artículo 248.2 CP). En este caso, a la vista de la redacción del artículo 197.3 tras la LO 5/2010 entienden ANARTE BORRALLO y DOVAL PAÍS[727] que hay que evitar la vulneración del *non bis in ídem* y, por tanto, considerar que no tiene especial significación autónoma la intrusión informática, siendo tan sólo una parte de la manipulación informática para conseguir la transferencia de activos. Atendida la posible insignificancia de la puesta en peligro de la intimidad o los datos personales, la consecuencia debe ser castigar tan sólo la estafa a efectos de evitar una sanción desproporcionada, excluyendo incluso el

---

[726] El artículo 189.1.a) establece que "*Será castigado con la pena de prisión de uno a cinco años: a) El que captare o utilizare a menores de edad o a personas con discapacidad necesitadas de especial protección con fines o en espectáculos exhibicionistas o pornográficos, tanto públicos como privados, o para elaborar cualquier clase de material pornográfico, cualquiera que sea su soporte, o financiare cualquiera de estas actividades o se lucrare con ellas*".

[727] ANARTE BORRALLO, E. y DOVAL PAIS, A., "Límites de la ley penal ...", *cit*., nota 24, p. 32.

concurso ideal por cuanto el injusto subyacente no resultaría suficiente para fundamentar una mayor pena.

Sin embargo, tras la reforma de la LO 1/2015, con la nueva redacción del artículo 197 *bis* 1 parece más acertado considerar que el intrusismo informático tiene ahora sustantividad propia, no siendo necesario el peligro para la intimidad o los datos, al no requerirse el efectivo acceso a datos o programas informáticos. Siendo esto así, la nueva configuración del delito referido al mero acceso al sistema, como delito de peligro y de resultado, donde existe un nuevo bien jurídico como es la seguridad de los sistemas informáticos, entiendo que llevaría a la consideración de un concurso de normas. En este sentido se sigue aquí el argumento de HURTADO ADRIÁN[728], que considera que con el intrusismo informático no es necesario averiguar el propósito del autor. Y ello porque la circunstancia de que el bien jurídico sea tan sólo la seguridad informática determina que este delito se encuentre en un peldaño inferior respecto a otros delitos para cuya comisión se haya tenido que pasar por vulnerar un sistema informático, hablando así de la progresión delictiva, es decir, concurso de normas que considera deberá solventarse conforme al principio de especialidad o alternatividad.

Y este mismo argumento a favor del concurso de normas, cabría en los delitos de defraudaciones de fluido eléctrico y análogas (artículos 255 y 256 CP), en los supuestos en que se accediese al

[728] HURTADO ADRIÁN, A., "Accesos informáticos ilícitos ...", *cit*., nota 145, p. 130.

sistema informático ajeno para cometer una defraudación utilizando energía o para hacer uso de un equipo terminal de comunicación.

Igualmente, frente al planteamiento de ANARTE BORRALLO y DOVAL PAÍS conforme al anterior artículo 197.3 CP, entendiendo que no tenía entidad suficiente para dar lugar a un injusto punible por su escasa incidencia en la intimidad cuando el acceso se produce para cometer un delito contra la propiedad intelectual del artículo 270 CP, especialmente cuando se accede para realizar copias ilegales de programas informático o se facilita el acceso ilegal en Internet[729], parece más acertada tras la reforma de la LO 1/2015 la consideración de que el intrusismo tiene entidad suficiente para fundamentar un concurso de normas.

---

[729] Artículo 270, apartados 1 y 2 CP: "1. *Será castigado con la pena de prisión de seis meses a cuatro años y multa de doce a veinticuatro meses el que, con ánimo de obtener un beneficio económico directo o indirecto y en perjuicio de tercero, reproduzca, plagie, distribuya, comunique públicamente o de cualquier otro modo explote económicamente, en todo o en parte, una obra o prestación literaria, artística o científica, o su transformación, interpretación o ejecución artística fijada en cualquier tipo de soporte o comunicada a través de cualquier medio, sin la autorización de los titulares de los correspondientes derechos de propiedad intelectual o de sus cesionarios. 2. La misma pena se impondrá a quien, en la prestación de servicios de la sociedad de la información, con ánimo de obtener un beneficio económico directo o indirecto, y en perjuicio de tercero, facilite de modo activo y no neutral y sin limitarse a un tratamiento meramente técnico, el acceso o la localización en internet de obras o prestaciones objeto de propiedad intelectual sin la autorización de los titulares de los correspondientes derechos o de sus cesionarios, en particular ofreciendo listados ordenados y clasificados de enlaces a las obras y contenidos referidos anteriormente, aunque dichos enlaces hubieran sido facilitados inicialmente por los destinatarios de sus servicios".*

Y el citado argumento también resultaría válido para otras conductas como las injurias o calumnias con publicidad (artículo 211 CP[730]), el descubrimiento de secretos de empresa (artículo 278.1 CP[731]), el delito de incitación al odio, hostilidad, discriminación o violencia (artículo 510.1.a CP[732]), daños a líneas de telecomunicaciones (artículo 560.1 CP[733]), enaltecimiento del terrorismo (artículo 578.1 CP[734]) o descubrimiento de secretos

---

730 Artículo 211 CP: "*La calumnia y la injuria se reputarán hechas con publicidad cuando se propaguen por medio de la imprenta, la radiodifusión o por cualquier otro medio de eficacia semejante.*".

731 Artículo 278.1 CP: "*El que, para descubrir un secreto de empresa se apoderare por cualquier medio de datos, documentos escritos o electrónicos, soportes informáticos u otros objetos que se refieran al mismo, o empleare alguno de los medios o instrumentos señalados en el apartado 1 del artículo 197, será castigado con la pena de prisión de dos a cuatro años y multa de doce a veinticuatro meses*.".

732 Artículo 510.1.a CP: "*1. Serán castigados con una pena de prisión de uno a cuatro años y multa de seis a doce meses: a) Quienes públicamente fomenten, promuevan o inciten directa o indirectamente al odio, hostilidad, discriminación o violencia contra un grupo, una parte del mismo o contra una persona determinada por razón de su pertenencia a aquél, por motivos racistas, antisemitas u otros referentes a la ideología, religión o creencias, situación familiar, la pertenencia de sus miembros a una etnia, raza o nación, su origen nacional, su sexo, orientación o identidad sexual, por razones de género, enfermedad o discapacidad*.".

733 Artículo 560.1 CP: "*Los que causaren daños que interrumpan, obstaculicen o destruyan líneas o instalaciones de telecomunicaciones o la correspondencia postal, serán castigados con la pena de prisión de uno a cinco años*".

734 Artículo 578.1 CP: "*El enaltecimiento o la justificación públicos de los delitos comprendidos en los artículos 572 a 577 o de quienes hayan participado en su ejecución, o la realización de actos que entrañen descrédito, menosprecio o humillación de las víctimas de los delitos terroristas o de sus familiares, se castigará con la pena de prisión de uno a*

relativos a la defensa nacional (artículo 598 CP[735]). Todo ello, tal y como señala HURTADO ADRIÁN[736], considerando que con la comisión de estos delitos en definitiva se está produciendo un intrusismo informático que superaría al mero *hacking* actualmente previsto en el artículo 197 *bis* 1 CP. Podemos entender por tanto que se produciría un intrusismo más sofisticado o complejo que el del precepto que nos ocupa, que fundamentaría el citado concurso de normas.

## *6. TOMA DE POSICIÓN.*

### *6.1 Aspecto subjetivo.*

El delito es común, pero el sujeto deberá actuar con conocimiento y voluntad de acceder sin autorización al sistema de información, vulnerando las medidas de seguridad, o mantenerse

---

*tres años y multa de doce a dieciocho meses. El juez también podrá acordar en la sentencia, durante el período de tiempo que él mismo señale, alguna o algunas de las prohibiciones previstas en el artículo 57.*".

[735] Artículo 598 CP: "*El que, sin propósito de favorecer a una potencia extranjera, se procurare, revelare, falseare o inutilizare información legalmente calificada como reservada o secreta, relacionada con la seguridad nacional o la defensa nacional o relativa a los medios técnicos o sistemas empleados por las Fuerzas Armadas o las industrias de interés militar, será castigado con la pena de prisión de uno a cuatro años".*

[736] HURTADO ADRIÁN, A., "Accesos informáticos ilícitos ...", *cit*., nota 145, p. 131.

dentro del sistema en contra de la voluntad de quien tenga el legítimo derecho a excluirlo, o bien, tras la reforma de la LO 1/2015, con conocimiento y voluntad de facilitarlo. Entiendo por ello que cabe el error de tipo, cuando recaiga sobre alguno de esos elementos, aunque resulta difícil pensar que suceda en la práctica, dada la exigencia del legislador de que se vulneren las medidas de seguridad para impedir el acceso, o el error de prohibición cuando tenga lugar sobre la antijuridicidad de la conducta. Parece difícil que puedan concurrir en la práctica cualquiera de los dos tipos de error, dada la exigencia de vulneración de las medidas de seguridad establecidas para impedir el acceso, salvo en el caso de facilitar estas conductas, donde podría concurrir el error de tipo si el sujeto creyese que está facilitando a otro sujeto el acceso al que se considera su sistema informático, siendo que se está accediendo ilícitamente a un sistema ajeno.

En cuanto al sujeto pasivo, cabe plantearse la falta de coincidencia entre el que es el titular del sistema y el de los datos contenidos. Desde mi punto de vista, si bien la cuestión era trascendente con el régimen de la LO 5/2010, en la medida en que se exigía el acceso a los datos o programas contenidos en el sistema informático, pudiendo quedar impune el acceso si el que accedía era el titular de ese contenido, tras la reforma de la LO 1/2015 el acceso castigado es al conjunto o parte de un sistema de información, por lo que será intrascendente la titularidad de los datos contenidos, y si se accede a ellos tendrá lugar un concurso de normas entre el artículo 197 *bis* 1 CP y, en su caso, con el artículo 197.2 CP.

### *6.2 Autoría y participación.*

En cuanto a las figuras de la autoría y la participación en el delito de *hacking*, se parte de la teoría del dominio del hecho iniciada por WELZEL[737], atendida la combinación entre elementos objetivos y subjetivos y su atención a la autoría mediata, aunque no resuelva el delito imprudente, cuestión que por otra parte no es relevante en el delito que nos ocupa dado la necesidad del dolo en el sujeto que lleva a cabo su ejecución.

Entiendo que en el acceso ilícito, siguiendo el criterio jurisprudencial y los planteamientos de la citada teoría, para que exista coautoría será preciso que el acceso se produzca de forma concertada entre varios sujetos, interviniendo cada uno de ellos en su ejecución como autores, todos ellos con un dominio del hecho consistente en el acceso ilícito o en el mantenimiento no autorizado en el sistema. Podría ser el caso del ataque simultáneo a un sistema informático convenido entre varios *hackers*, sobrepasando todos las medidas de seguridad dispuestas por su titular para proteger el sistema informático, logrando acceder al sistema gracias a los ataques de los otros y sin los cuales a su vez no podrían haber accedido; o el caso en el que permaneciesen en el sistema al que han accedido de forma autorizada varios sujetos una vez retirada la autorización del titular

[737] WELZEL, H., *Estudios de Derecho penal ...*, *cit*., nota 340, pp. 88, 89, 96 y 101.

que no se apercibe de ello precisamente porque ninguno de esos sujetos lo ha abandonado.

Parece también posible la autoría mediata en estos delitos, como sucedería en el caso de que el dominio del hecho se llevase a cabo mediante coacción, por violencia o amenazas sobre un sujeto para que realice el acceso ilícito al sistema informático o se mantenga en el sistema sin autorización, o bien induciéndole a error o aprovechando la situación de error en la que se encuentra, sea error de tipo o por encontrarse en una situación de inimputabilidad como pudiera ser la anomalía o alteración psíquica que sufriese el sujeto/instrumento, situación de la que se aprovecharía el autor mediato para cometer el delito de *hacking* a través de este instrumento.

En cuanto a la participación, siguiendo a QUINTERO OLIVARES, distingo entre la inducción, la complicidad necesaria y la no necesaria[738] en el intrusismo informático.

Así, la inducción la analizo partiendo del criterio jurisprudencial, reflejado entre otras en la citada STS de 16 de marzo de 2015[739], de considerarla como influjo psíquico, logrado de diversas formas posibles, que el inductor despliega sobre otras personas (autores materiales) al objeto de que ejecuten un delito concreto y en relación también con una víctima concreta, se plantearían supuestos

[738] QUINTERO OLIVARES, G., con la colaboración de MORALES PRATS, F., *Parte general ..., cit*., nota 464, p. 657.

[739] STS, Sala Segunda, de 16 de marzo de 2015, cit., nota 675.

tales como el del sujeto que influye en otro para que lleve a cabo el acceso ilícito a un sistema de información, siempre y cuando el sujeto que lo ejecuta no estuviese ya decidido a cometer el delito antes, y siendo necesaria la efectiva ejecución, puesto que en caso contrario estaríamos en el supuesto de la proposición previsto en el artículo 17.2 CP.

Conviene precisar que dado el sistema de *numerus clausus* en el CP respecto a la proposición, provocación y conspiración para delinquir, puesto que no existe una tipificación expresa de estas conductas, no existiría castigo para quien las llevase a cabo. No obstante, puesto que el legislador equipara al provocador con el inductor cuando el delito llega a ejecutarse, de tal manera que en el supuesto de que un sujeto incitase directamente *"por medio de la imprenta, la radiodifusión o cualquier otro medio de eficacia semejante, que facilite la publicidad, o ante una concurrencia de personas, a la perpetración de un delito"* de *hacking*, sería castigado sólo si la provocación de este delito estuviese expresamente tipificada (artículo 18 CP), por lo que en principio la conducta del provocador no estaría castigada al no existir esta tipificación. Sin embargo, tal y como establece el mismo precepto, "*Si a la provocación hubiese seguido la perpetración del delito, se castigará como inducción"*.

Por lo que respecta a la participación en el delito, en la cooperación necesaria opto por seguir el criterio jurisprudencial que aglutina las distintas teorías para distinguirla de la coautoría, donde el coautor dirige su acción a la realización del tipo con dominio de la

acción, mientras que el cooperador necesario en estos delitos será quien colabore en el acceso al sistema informático con una conducta sin la cual no se podría haber accedido o permanecido dentro de él (teoría de la *conditio sine qua non*, así en el ejemplo de abrir la puerta blindada de la habitación donde se encuentra el ordenador al que se pretende acceder o provocando la distracción del titular del sistema para que otro sujeto se mantenga en él), aportando algo que no es fácil de obtener de otro modo (teoría de los bienes escasos, por ejemplo aportando una copia de la llave del almacén donde se encuentra el sistema informático al que se va a acceder o accediendo a un sistema mediante las claves de acceso de las que tiene conocimiento para que así otro sujeto pueda permanecer en él de forma no autorizada), o cuando el que colabora puede impedir la comisión del delito retirando su concurso (teoría del dominio del hecho, por ejemplo el que facilita el cableado ethernet para poder acceder al sistema informático y puede retirar en cualquier momento el cable impidiendo la comisión del delito).

No obstante, considero que tras la reforma del artículo 197 *bis* 1 CP por la LO 1/2015, la distinción práctica entre la autoría y la cooperación necesaria en el delito de acceso ilícito a los sistemas informáticos va a difuminarse en la medida en que conforme al citado artículo serán autores tanto el que "*acceda*" como el que "*facilite a otro el acceso*".

Por otra parte, entiendo que podrán plantearse problemas a la hora de distinguir la complicidad de la cooperación necesaria, razón

por la cual, atendiendo una vez más al criterio del Tribunal Supremo, establecido entre otras en su STS de 4 de febrero de 2015[740], el cómplice del delito de acceso ilícito a un sistema informático no tendría dominio del hecho, pero realizaría actos accesorios o periféricos, con conocimiento del propósito criminal del autor y voluntad de contribuir en ese acceso. Por tanto, una vez más resulta prácticamente muy difícil pensar en algún supuesto de complicidad en el delito del artículo 197 *bis* 1 CP, por cuanto tras la citada reforma de la LO 1/2015 el legislador ha equiparado las conductas entre el que "*acceda*" y el que "*facilite a otro el acceso*", ampliando de forma criticable los supuestos de autoría a los supuestos que, conforme a la doctrina y jurisprudencia expuesta, tendrían la consideración de participación.

Así pues, de acuerdo con la diferencia entre las conductas de facilitar el acceso del artículo 197 *bis* 1 y las de facilitar el acceso por alguno de los medios del artículo 197 *ter* CP, que los casos de complicidad se van a reducir de forma residual a las conductas de facilitar el acceso que no estén previstas en esos dos artículos. Así pues, entiendo que la complicidad se limitaría a los casos en los que el sujeto ayuda al acceso al sistema informático siempre que no lo hiciera facilitando los instrumentos del artículo 197 *ter* CP, excluyendo así la aplicación de este precepto como autor y, además, el acceso no tuviese éxito, eludiendo de esta forma la autoría del artículo

740 STS de 4 de febrero de 2015, *cit*., nota 678.

197 *bis* 1 CP, que como hemos visto queda reducido a los supuestos de facilitar el acceso cuando éste no llega a producirse para así distinguirlo de las conductas del artículo 197 *ter* CP.

Por último, para la complicidad en el caso de las conductas de mantenimiento no autorizado en el sistema, siguiendo el citado criterio jurisprudencia, considero que se deberían relizar actos accesorios o periféricos, con conocimiento del propósito criminal del autor y voluntad de contribuir a esa permanencia por algún medio no encuadrable en el artículo 197 *ter* CP.

### *6.3 Iter criminis*.

En el delito que nos ocupa, de peligro concreto y de resultado, se anticipa la barrera de protección de los bienes jurídicos que puedan verse afectados, y lo hace todavía más tras la reforma de la LO 1/2015, donde ya no es necesario acceder a datos o programas contenidos en el sistema de información, sino que es suficiente el acceso a todo o parte del mismo. Por ello, si el anterior régimen introducido por la LO 5/2010 había sido criticado como hemos visto atendidos los bienes jurídicos que pudieran verse afectados por el acceso a datos o programas informáticos, más criticable podría entenderse la anticipación de la tutela de los bienes jurídicos al mero acceso al sistema con independencia de su contenido. Sin embargo, parece que el legislador ha querido dar un paso más en la

configuración del denominado domicilio informático y dotar de mayor protección a los numerosos bienes jurídicos que con el intrusismo informático o tras el acceso o mantenimiento pueden verse afectados, algo que por otra parte entiendo comprensible y acorde con el ritmo acelerado de las nuevas tecnologías y el fácil acceso a mecanismos y programas que hoy día hacen posible para cualquiera llevar a cabo ese intrusismo.

En el presente Capítulo se ha analizado la fase externa del delito, por resultar irrelevante jurídicamente la interna, intentando delimitar la fase de ejecución del delito a efectos de punición de la conducta o no. Así, he optado por seguir la doctrina de CARRARA[741] por resultar la más sencilla a efectos de delimitar los actos preparatorios del *hacking*, entendiendo así que cuando el sujeto realice actos que por sí mismos evidencien unívocamente la intención de acceder o mantenerse ilícitamente en el sistema o facilitar el acceso, estaremos en la fase de ejecución del delito tipificado en el artículo 197 *bis* 1 CP, mientras que cuando el acto que se realice pueda llevar a la ejecución del delito o a cualquier otro acto no ofensivo, será un acto preparatorio impune, como sucedería en los ejemplos del caso del sujeto que sin autorización comprueba las medidas de seguridad de un sistema informático ajeno sin quebrantarlas; o en el supuesto que elabora un generador de claves, sin utilizarlo ni ofrecerlo, que permite, si se llega a ejecutar, la generación de una clave para poder acceder al

741 CARRARA, F., *Programa de Derecho Criminal …*, *cit*., nota 513, pp. 247 y 248.

sistema informático propio en el caso de bloqueo accidental pero que igualmente fuera válido para poder acceder ilícitamente a un sistema ajeno.

Por otra parte, el legislador ha decidido tipificar expresamente los actos preparatorios de estos delitos en los artículos 197 *bis* 1 y 197 *ter* CP, produciéndose así un *iter criminis* expansivo, donde se anticipa la tutela de la seguridad de los sistemas informáticos incluso al momento de facilitar la conducta, bien aportando alguno de los instrumentos que se citan en el artículo 197 *ter* CP, o bien facilitándola de cualquier otra forma conforme al artículo 197 *bis* 1 CP, siempre que como ya se ha apuntado, en este último caso se produzca un efectivo acceso al sistema, por coherencia penológica con la conducta de acceso.

En cuanto a las resoluciones manifestadas consistentes en la provocación, conspiración y proposición, carecen de castigo en el caso del intrusismo informático del artículo 197 *bis* 1 CP, sin perjuicio del castigo al inductor en la forma ya mencionada. De igual forma, entiendo que por los mismos motivos en principio no estaría castigada la apología, al ser una forma de provocación y no estar expresamente penada la provocación del acceso ilícito o mantenimiento no autorizado en un sistema de información, por lo que tampoco podrá serlo la apología de estos delitos, salvo que que se produjese la efectiva perpetración del delito tras la incitación directa, hecho que podría reconducirse a la inducción conforme al citado artículo 18.2 CP.

Por lo que respecta a la tentativa, he distinguido entre la modalidad acabada e inacabada por una parte, y el desistimiento y el arrepentimiento activo por otra. Para diferenciarlos he seguido el criterio jurisprudencial reflejado en la STS de 2 de noviembre de 2011, es decir, entender que existirá tentativa acabada del acceso ilícito al sistema informático cuando "*los actos realizados, los instrumentos utilizados y la mecánica comisiva hubieran podido producir objetivamente el resultado perseguido según el plan del autor*"[742].

De esta forma, entiendo, siguiendo el criterio de HURTADO ADRIÁN[743], que será posible que el acceso no se produzca, porque una vez iniciado el proceso el sujeto no sea capaz de quebrantar las medidas de seguridad (tentativa inacabada) o porque vulneradas no se consiga acceder al sistema de información (tentativa acabada), con las consecuencias del artículo 62 del CP, y además, conforme al planteamiento expuesto del Tribunal Supremo, para ello se habrán considerado los actos, instrumentos y la mecánica empleada por el sujeto para llevar a cabo el acceso, por cuanto si con estos elementos se hubiese podido producir objetivamente el resultado del acceso al sistema pretendido, estaremos ante la tentativa acabada del delito del artículo 197 *bis* 1 CP, mientras que si no se hubiese podido alcanzar el resultado, será la modalidad inacabada.

---

742 STS de 2 de noviembre de 2011, *cit*., nota 700.

743 HURTADO ADRIÁN, A., "Accesos informáticos ilícitos ...", *cit*., nota 145, p. 126.

En cuanto a la distinción entre desistimiento o arrepentimiento activo en el acceso ilícito al sistema, siguiendo el planteamiento de la STS de 7 de junio de 1985, considero que si el sujeto que inicia el delito de *hacking*, de forma voluntaria, personal y definitiva, y sin ningún obstáculo insuperable que le impidiese acceder al sistema, decide no culminar todos los actos de ejecución, estaremos ante el desistimiento, tal y como sucedería en el ejemplo del que se conecta remotamente a otro sistema para acceder ilícitamente y ejecutados parte de los programas que permiten quebrantar las medidas de seguridad establecidas, decide voluntariamente dejar de ejecutar el que le facilitaría la clave de acceso al sistema informático ajeno. En caso contrario, siguiendo el criterio anterior de la tentativa inacabada e inacabada, si ha surgido un obstáculo insuperable para alcanzar ese resultado, impidiendo la ejecución de todos los actos, como sucedería si el último programa resulta no ser ejecutable e inesperadamente el sujeto no puede ejecutar el programa para acceder, no existirá un desistimiento, sino una tentativa inacabada. El sujeto no accederá porque no puede acceder.

Pero si se han ejecutado todos los actos para el acceso, y el resultado no se produce por la decisión del sujeto que realiza ese acceso, entiendo que tendrá lugar el arrepentimiento activo, lo que sucedería en el citado ejemplo del que se conecta remotamente a otro sistema para acceder ilícitamente y ejecutados los programas que permiten quebrantar las medidas de seguridad, habiendo obtenido ilícitamente la clave de acceso a ese sistema, e introducida, mientras carga el acceso decide apagar su ordenador y, por tanto, no acceder.

Por el contrario, si no ha sido el sujeto quien ha llevado la actuación para evitar que el resultado se produzca, entiendo que se producirá la tentativa acabada, lo que en el ejemplo citado, sucedería si el titular del sistema al que se pretende acceder se cerciora de que se están tratando de quebrantar la seguridad de su ordenador y decidiera cambiar las medidas de seguridad y además reforzarlas, hasta tal punto de resultar un escollo insalvable para el sujeto que pretendía acceder.

Considero que sería posible la tentativa inidónea, como sucedería si se pretendiera acceder desde un *e-reader* al sistema del CNI, y el delito imposible, por ejemplo, un sujeto entra en un edificio para llegar hasta el habitáculo donde supuestamente se encuentra su sistema informático y allí acceder al mismo, pero una vez en el lugar comprueba que el edificio no cuenta con sistema informático.

Por útlimo, atendidas las características de las conductas de mantenimiento por una parte, donde la consumación se determina en cada caso atendiendo al momento hasta donde el sujeto estaba autorizado y la capacidad para poner en peligro concreto el sistema, y las de facilitar el acceso por otra parte, donde si no se alcanza el acceso la conducta se encuadrará en el artículo 197 *ter*, desde mi punto de vista será difícil que en la práctica pueda darse la tentativa en alguno de estos supuestos.

### *6.4 Relaciones concursales.*

Tal y como se ha manifestado, la reforma llevada a cabo por la LO 1/2015 implica un adelantamiento todavía mayor de las barreras de protección de los bienes jurídicos con la nueva regulación del delito de *hacking*.

El citado adelantamiento y redacción del artículo 197 *bis* 1 CP puede conllevar numerosos problemas prácticos por su concurrencia con otros delitos. Así, considero que el hecho de que se facilite el acceso a un sistema informático, conducta que nos ocupa, puede confundirse fácilmente con la del artículo 197 *ter* a "*de cualquier otro modo, facilite a terceros*", lo que llevará a resolver el concurso atendiendo al criterio de que efectivamente se produzca el acceso, de tal manera que si se facilita la conducta de *hacking* y el acceso se produce, por coherencia penológica entre acceder y facilitar sería encuadrable la conducta en el artículo 197 *bis* 1, mientras que si no se llega a producir el acceso, dada la especialidad de los medios en el artículo 197 *ter*, se debería resolver el concurso a favor de la aplicación de este último precepto. Será distinto el caso en el que el sujeto facilita medios para la comisión del *hacking* y a su vez también lleva a cabo el delito del artículo 197 *bis* 1. En estos casos parece más adecuado considerar la conducta como un delito continuado de acceso ilícito.

En los casos que fuese necesario un acceso físico al espacio (morada) donde se encuentra el sistema informático, como infracción más grave, absorberá al allanamiento de morada con las consecuencias del artículo 77.3 CP. Cuestión distinta será acceder a un sistema informático que permita el control monitorizado del interior de una vivienda o establecimiento. En estos casos la concurrencia entre el allanamiento de morada y el *hacking* será meramente aparente, puesto que para el allanamiento se requiere efectiva entrada (o permanencia), por lo que accediendo al sistema informático no tendría lugar el delito de allanamiento de morada.

Por su parte, cuando el sujeto accediese al sistema informático apoderándose de datos reservados o sin estar autorizado acceda a ellos dará dar lugar al concurso de normas entre el delito del artículo 197 *bis* 1 CP y el del artículo 197.2 CP, quedando absorbido por éste último, de esta forma, tal y como indican ANARTE BORRALLO y DOVAL PAÍS[744] con ocasión del artículo 197.3 en su redacción dada tras la LO 5/2010, ante la identidad de bienes jurídicos o al menos de línea de ataque, entiendo que se aplicaría el criterio de la consunción del delito cuyo umbral típico se ubica más lejos de la afección al bien jurídico protegido.

En los supuestos en que el instrusismo sea paso previo a la comisión del delito de daños informáticos regulado en el artículo 264 CP, la tentativa del delito de daños cuando no se llega a causar el daño

[744] ANARTE BORRALLO, E. y DOVAL PAIS, A., "Límites de la ley penal ...", *cit*., nota 24, p. 31.

por causas independientes a la voluntad del autor, considero que constituiría un delito consumado de *hacking*, al configurarse como un delito autónomo de peligro concreto que conllevaría mayores penas que la tentativa de daños, a la que absorbería. Si el daño pretendido fuese efectivamente causado una vez producido el acceso, se producirá el concurso ideal en su versión medial, en cuanto el acceso se configura como un medio necesario para causar el daño, que absorbería al *hacking* con las consecuencias del artículo 77.3 CP. Otro caso sería el que una vez consumado el intrusismo, se decidiera causar daños informáticos o, al revés, cuando provocados daños informáticos, se realizase el acceso ilícito con posterioridad, en cuyo caso, siguiendo la opinión expuesta de ANARTE BORRALLO y DOVAL PAÍS[745], entiendo que tendría lugar un concurso real.

Por último, si consideramos el acceso ilícito a un sistema de información como paso previo a la comisión de otros delitos, son numerosas las situaciones concursales que se pueden producir. Así, los casos del delito de *grooming* (artículo 183 *ter*), donde considero conforme a los citados autores que se produciría un concurso real de delitos, por cuanto no podría considerarse el acceso al sistema informático como un medio que fuera únicamente dirigido al contacto con el menor, sino que al menos causaría también un peligro de la intimidad y datos personales del menor. A la misma conclusión se llegaría si el acceso al sistema informático ajeno fuese para la

745 *Ibíd.,* p. 33.

captación de menores con finalidad exhibicionista o pornográfica, prevista en el artículo 189 CP.

Si el acceso ilícito fuese para la comisión de un delito de estafa informática (artículo 248.2 CP), en este caso, frente al planteamiento que hacen a la vista de la redacción del artículo 197.3 tras la LO 5/2010 ANARTE BORRALLO y DOVAL PAÍS[746], que consideran que hay que evitar la vulneración del *non bis in ídem* y, por tanto, no teniendo especial significación autónoma la intrusión informática, siendo tan sólo una parte de la manipulación informática para conseguir la transferencia de activos, atendida la posible insignificancia de la puesta en peligro respecto a la intimidad o los datos personales, la consecuencia debe ser castigar tan sólo la estafa a efectos de evitar una sanción desproporcionada, excluyendo incluso el concurso ideal por cuanto el injusto subyacente no resultaría suficiente para fundamentar una mayor pena, considero que, tras la reforma de la LO 1/2015, con la nueva redacción del artículo 197 *bis* 1 parece más acertado entender que el intrusismo informático tiene ahora sustantividad propia. Por tanto, no es necesario el peligro para la intimidad o los datos, al no requerirse el efectivo acceso a datos o programas informáticos y, por tanto, la nueva configuración del delito referido al mero acceso al sistema, como delito de peligro y de resultado, donde existe un nuevo bien jurídico como es la seguridad de los sistemas informáticos, daría lugar a un concurso de normas que se resolvería a favor del delito de estafa. Para ello sigo el argumento

746 *Ibíd*., p. 32.

expuesto por HURTADO ADRIÁN[747], que considera que con el intrusismo informático no es necesario averiguar el propósito del autor. Y ello porque la circunstancia de que el bien jurídico sea tan sólo la seguridad informática, determina que este delito se encuentre en un peldaño inferior respecto a otros delitos para cuya comisión se haya tenido que pasar por vulnerar un sistema informático, hablando así de la progresión delictiva, es decir, concurso de normas que deberá solventarse conforme al principio de especialidad o alternatividad.

Y este mismo argumento a favor del concurso de normas, entiendo que cabría en los delitos de defraudaciones de fluido eléctrico y análogas (artículos 255 y 256 CP), en los casos en que se accediese al sistema informático ajeno para cometer una defraudación utilizando energía o para hacer uso de un equipo terminal de comunicación. Igualmente, frente al citado planteamiento de ANARTE BORRALLO y DOVAL PAÍS conforme al anterior artículo 197.3 CP, considerando que no tenía entidad suficiente para dar lugar a un injusto punible por su escasa incidencia en la intimidad cuando el acceso se produce para cometer un delito contra la propiedad intelectual del artículo 270 CP, especialmente cuando se accede para realizar copias ilegales de programas informático o se facilita el acceso ilegal en Internet, entiendo que tras la reforma de la LO 1/2015 la consideración de que el intrusismo tiene entidad suficiente para fundamentar un concurso de normas. Y el citado argumento también

[747] HURTADO ADRIÁN, A., "Accesos informáticos ilícitos ...", *cit*., nota 145, p. 130.

resultaría válido para otras conductas como las injurias o calumnias con publicidad (artículo 211 CP), el descubrimiento de secretos de empresa (artículo 278.1 CP), incitación al odio, hostilidad, discriminación o violencia (artículo 510.1.a CP), daños a líneas de telecomunicaciones (artículo 560.1 CP), enaltecimiento del terrorismo (artículo 578.1 CP) o descubrimiento de secretos relativos a la defensa nacional (artículo 598 CP). Todo ello siguiendo el planteamiento de HURTADO ADRIÁN[748] y considerando que con la comisión de estos delitos en definitiva se está produciendo un intrusismo informático que superaría al mero *hacking* actualmente previsto en el artículo 197 *bis* 1 CP. Considero por tanto que se produciría un intrusismo más sofisticado o complejo que el del precepto que nos ocupa, que fundamentaría el citado concurso de normas.

[748] *Ibíd*., p. 131.

# CAPÍTULO V.

# LOS TIPOS AGRAVADOS DEL *HACKING*.

*1. INTRODUCCIÓN.*

Una vez expuestos los elementos de la figura de *hacking* incluidos en el artículo 197 *bis* 1 del CP y la ejecución del delito, se analiza en el presente apartado el tipo agravado del artículo 197 *quater*, incorporado al Código Penal por la LO 1/2015, y el del artículo 198.

En primer lugar, en el artículo 197 *quater* se dispone:

"*Si los hechos descritos en este Capítulo se hubieran cometido en el seno de una organización o grupo criminal, se aplicarán respectivamente las penas superiores en grado".*

Se pueden considerar como antecedentes remotos de la delincuencia organizada las agravantes genéricas previstas en el artículo 106 del Código Penal de 1822, que establecía "*En todo delito ó culpa para la graduación expresada en los dos primeros artículos se tendrán por circunstancias agravantes, además de las que esprese la ley en los casos respectivos, las siguientes: (...) Quinta: el mayor número de personas que concurran al delito*"; o las reguladas en el artículo 10, apartados 12 y 13 del Código Penal de 1944, ubicado en su Libro Primero dedicado a las "*Disposiciones generales sobre los delitos y faltas, las personas responsables y las penas*", en el que se disponía que "*Son circunstancias agravantes: (...) 12. Ejecutarlo con auxilio de gente armada o de personas que aseguren o proporcionen la impunidad. 13. Ejecutarlo de noche, en despoblado o en cuadrilla.*

*Hay cuadrilla, cuando concurren a la comisión del delito más de tres malhechores armados*".

Sin embargo, el artículo 197 *quater* CP adapta la previsión del anterior artículo 197.8, introducido como novedad en el Código Penal por la LO 5/2010 y relativo a la comisión de estos delitos en el seno de una organización o grupo criminal, configurándose así como una agravante específica, regulada en su parte especial.

El precepto a su vez trae causa de las disposiciones internacionales que han pasado a formar parte del ordenamiento jurídico español. En concreto, la Convención de las Naciones Unidas contra la Delincuencia Organizada Transnacional, la DM 2005/222/JAI y la Directiva 2013/40/UE, tal y como se verá en el siguiente punto.

En este sentido, siguiendo el criterio de VELASCO NUÑEZ[749], estos tipos de asociaciones necesitan la concurrencia de una serie de requisitos a los que se hará referencia en el presente Capítulo, distinguiendo este autor entre los que son de naturaleza esencial y los de tipo adjetivo, es decir, no nucleares, pero sí reafirmantes de la agravación, configurándose como una circunstancia de agravación específica que como tal requiere de una interpretación restrictiva. Además, como señala CUERDA ARNAU, presentan unos elementos comunes, como son estar formadas por más de dos

[749] VELASCO NUÑEZ, E., "Delitos informáticos …", *cit*., nota 665, p. 5.

personas y la finalidad de cometer delitos[750], y como indica ROMA VALDÉS[751], comparten el elemento subjetivo doloso, por el que el sujeto debe conocer y prestar su voluntad a los elementos objetivos, no admitiendo el delito su forma culposa.

En consecuencia, aunque como dice GONZÁLEZ CUSSAC el legislador distingue en estos casos dos niveles de concierto de personas para cometer delitos, es decir, organizaciones y grupos criminales en sus artículos 570 *bis* y *ter*[752], sin embargo, conviene aquí precisar que en el artículo 197 *quater* se ubican en el mismo nivel, tal y como veremos en el presente Capítulo. No obstante, el caso que nos ocupa es un supuesto distinto de aquellos en los que el responsable de estas conductas sea una persona jurídica, a la que se hará referencia más adelante y de la que se ocupa el artículo 197 *quinquies*, sustituyendo al anterior artículo 197.3, párrafo segundo.

La reforma de la LO 1/2015 ha modificado la estructura del artículo 197 CP, no sólo en lo que se refiere a la ubicación del tipo

---

750 CUERDA ARNAU, M. L., "Delitos contra el orden público", en GONZÁLEZ CUSSAC, J.L. (Coord.), y VVAA. *Derecho penal. Parte especial*, ed. Tirant Lo Blanch, Valencia, 2016, pp. 758 y 759.

751 ROMA VALDÉS, A., "El delito de organizaciones y grupos criminales", en *Estudios jurídicos*, nº 2012, ed. Ministerio de Justicia, Centro de Estudios Jurídicos, Madrid, 2012, p. 15, disponible en http://www.academia.edu/2394755/EL_DELITO_DE_ORGANIZACIONES_Y_GRUPOS_CRIMINALES, consultado el 9 de abril de 2017.

752 GONZÁLEZ CUSSAC, J. L., "Estrategias legales frente a las ciberamenazas", en *Cuadernos de estrategia (Ministerio de Defensa)*, ed. Ministerio de Defensa: Instituto Español de Estudios Estratégicos, nº 149, Madrid, 2011, p. 106.

básico del *hacking*, sino por cuanto ha despenalizado la mayoría de los tipos agravados previstos en la LO 5/2010 en relación con estas conductas, cuyo estudio no constituye el objeto de este trabajo: (i) difundir, revelar o ceder a terceros los datos o hechos descubiertos o las imágenes captadas, que pasan del anterior 197.4 al nuevo artículo 197.7; (ii) la realización del acceso ilícito por parte de las personas encargadas o responsables de los ficheros, soportes informáticos, electrónicos o telemáticos, archivos o registros, que pasan del artículo 197.5 al nuevo artículo 197.4, referido ahora sólo a las conductas del artículo 197, apartados 1 y 2; (iii) que los hechos 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, que se incorporan desde el artículo 197.6 al nuevo artículo 197.5; y (iv) que se lleve a cabo con ánimo de lucro, que pasan del anterior artículo 197.7 al nuevo 197.6.

Así pues, el artículo 197 *quater* incorpora el único tipo agravado aplicable a todas las conductas comprendidas en el Capítulo, comprendiendo también los accesos ilícitos al sistema de información.

Por ello, estando referido el citado tipo agravado a las conductas de acceso ilícito al conjunto o parte del sistema de información, se trata en el presente Capítulo su fundamento y breve exposición, pues un análisis pormenorizado exigiría de una obra separada.

En segundo lugar, se analizan los elementos que diferencian el tipo agravado previsto en el artículo 198 CP del tipo básico al que nos hemos referido en los anteriores apartados, precepto que establece:

"*La autoridad o funcionario público que, fuera de los casos permitidos por la Ley, sin mediar causa legal por delito, y prevaliéndose de su cargo, realizare cualquiera de las conductas descritas en el artículo anterior, será castigado con las penas respectivamente previstas en el mismo, en su mitad superior y, además, con la de inhabilitación absoluta por tiempo de seis a doce años"*.

El análisis del artículo 198 CP puede interpretarse referido, entre otras, a las conductas de *hacking* llevadas a cabo por autoridad o funcionario público, concurriendo las circunstancias que se expondrán en este Capítulo.

Sin embargo, conviene tener presente en todo momento que la LO 1/2015 no ha modificado el citado artículo 198 y, por tanto, el precepto sigue refiriéndose a la autoridad o funcionario público que "*realizare cualquiera de las conductas descritas en el artículo anterior*", y si bien tras la reforma de la LO 5/2010 el artículo comprendía las conductas del artículo 197, en cuyo apartado 3 se encontraba el acceso ilícito a los sistemas informáticos, ahora el "*artículo anterior*" es el mencionado 197 *quinquies*, relativo a la responsabilidad de las personas jurídicas. Dicho en otras palabras, se ha modificado el artículo 197 pero se ha dejado intacto el artículo 198. De esta forma parece evidente la errata del legislador en la LO 1/2015

manteniendo la misma redacción del artículo 198, por cuanto para evitar problemas interpretativos debería haber referido el precepto a "los artículos anteriores" en los que ahora se desgrana el anterior artículo 197. En consecuencia, la referencia del artículo 198 se interpretaría con remisión a todas las conductas del anterior artículo 197 y, de esta forma, comprendería también los supuestos del acceso ilícito a un sistema de información regulados en el artículo 197 *bis*. Este planteamiento resulta de una interpretación lógica del precepto que llevaría a comprender el delito de *hacking*. Sin embargo, conviene recordar que el principio de legalidad rige en nuestro ordenamiento jurídico, de tal forma que como señalaba ANTÓN ONECA[753], la legislación penal es un ordenamiento cerrado, sin lagunas que puedan ser llenadas por los tribunales en lo referente a definición de delitos y aplicación de penas. Este principio excluye la posibilidad de aplicar analógicamente el artículo 198 CP a un supuesto que regulaba tras la LO 5/2010 pero que tras la LO 1/2015 no contempla expresamente, como es el del artículo 197 *bis* 1, por cuanto conforme al artículo 4.1 CP "*Las leyes penales no se aplicarán a casos distintos de los comprendidos expresamente en ellas".*

Esperaremos a la respuesta práctica de los tribunales en su aplicación, pareciendo lógica la voluntad del legislador de incluir las conductas de *hacking*, puesto que con la reforma de la LO 5/2010 estas conductas eran reguladas en el artículo 197.3 CP y el artículo 198 CP las comprendía, razón por la cual no se entiende, porque no

753 ANTÓN ONECA, J., *Derecho Penal …*, *cit*., nota 443, p. 110.

hay motivo para ello, que tras la reforma de la LO 1/2015, con el desglose del anterior artículo 197 en varios preceptos, ahora se excluya el artículo 197 *bis* 1 (anterior artículo 197.3) del ámbito del artículo 198 CP. De esta forma, parece que deberán ser los tribunales quienes por la vía del artículo 4.2 CP[754] y precisamente en estricto cumplimiento del principio de legalidad, no apliquen el artículo 198 CP en relación con el artículo 197 *bis* pero interesen al Gobierno la corrección de la errata a efectos de que en el futuro pueda aplicarse el artículo 198 CP también a esos delitos de *hacking*. Ello, por cuanto como indica GUARDIOLA GARCÍA[755], la corrección de errores debe provenir de quien tiene legitimidad para ello, es decir, de las Cortes Generales, que son quienes pueden dictar normas penales, y además por el procedimiento legislativo con más garantías. Razón por la cual esa modificación del precepto ni siquiera podría hacerse con una

---

754 El artículo 4.2 CP dispone que "*En el caso de que un Juez o Tribunal, en el ejercicio de su jurisdicción, tenga conocimiento de alguna acción u omisión que, sin estar penada por la Ley, estime digna de represión, se abstendrá de todo procedimiento sobre ella y expondrá al Gobierno las razones que le asistan para creer que debiera ser objeto de sanción penal.".*

755 GUARDIOLA GARCÍA, J., "Corrección de errores en el BOE y principio de legalidad en materia penal", *La Ley Penal, nº 10, Sección Legislación aplicada a la práctica*, ed. La Ley, noviembre 2004, p. 2. Si bien en el caso concreto el autor se refiere a la LO 15/2003, por la que se reformaban los artículos 234 y 244 CP, diciendo que disponía la modificación del "art. 234" y el "apartado 1 del art. 244", sin introducir ni en uno ni en otro el párrafo segundo en cuestión, derogandolos así tácitamente, razón por la cual debían ser las Cortes Generales quienes debían reformar de nuevo esos preceptos y no el BOE de 16 de marzo de 2004 con el que se intentaba solucionar el error, por cuanto el BOE puede corregir errores de transcripción propios, pero no el contenido de la LO 15/2003 aprobada.

nueva publicación en el BOE, porque por esta vía sería posible enmendar errores de transcripción propios, pero no modificar un precepto, en nuestro caso el artículo 198 CP para referirlo al artículo 197 *bis* 1.

Por tanto, con estos matices, en los siguientes apartados también se hace referencia a los elementos exigidos en el artículo 198 CP, partiendo de que con la regulación de estas conductas ya no sólo se tutela la integridad o seguridad de los sistemas informáticos, sino también el interés de la Administración y el de la sociedad en general respecto de la correcta actuación de las autoridades y funcionarios públicos[756].

## *2. EL TIPO AGRAVADO DEL ARTÍCULO 197 QUATER.*

### *2.1 Fundamento del tipo agravado.*

[756] La STS, Sala Segunda, de 23 de septiembre de 2015, nº 534/2015, recurso 462/2015, Pte. Excmo. Sr. D. Miguel Colmenero Menéndez de Luarca, en su FD 1º declara que "*los bienes jurídicos protegidos por el artículo 198 no se reducen al interés privado en mantener la propia privacidad, sino que se extienden al de la Administración y al de la sociedad en general respecto de la correcta actuación de las autoridades y funcionarios públicos*".

La criminalidad organizada puede definirse con VELASCO NÚÑEZ[757] como la manifestación de la participación criminal en el delito con fórmulas de concertación delictiva que superan la mera individualidad. En consecuencia, es un fenómeno que se ha visto favorecido con las nuevas tecnologías, por cuanto, siguiendo al citado autor, es necesario mantener al grupo en contacto constantemente, abren la posibilidad de atacar a bienes jurídicos tradicionales a través de ellas (como en el caso del acceso a las fotografías de una persona ubicadas en su ordenador habiendo vulnerado previamente sus medidas de seguridad) o incluso permiten dañar o destruir estos nuevos instrumentos (p.ej. con la introducción de un virus informático en el sistema una vez se accede a su contenido).

Por ello, siguiendo a MIRÓ LLINARES el motivo de la agravante consiste en prevenir y mejorar la lucha contra la criminalidad organizada a través de las nuevas tecnologías[758], y siguiendo a MORALES PRATS, podemos entender que en estas conductas se produce un incremento en el desvalor de la acción, por la mayor peligrosidad *ex ante*, y en el desvalor del resultado, por la mayor afectación del bien jurídico *ex post*[759], fundamentando así el mayor castigo, añadiendo con SIERRA LÓPEZ que en estas conductas existe un mayor desvalor de la acción por la mayor

---

757 VELASCO NUÑEZ, E., "Delitos informáticos ...", *cit*., nota 665, p. 1.

758 MIRÓ LLINARES, F., "Los Delitos Informáticos ...", *cit*., nota 108, p. 155.

759 MORALES PRATS, F., "Delitos contra la intimidad ...", *cit*., nota 489, p. 480.

facilidad que supone realizar estas conductas a través de una organización o grupo criminal[760].

Tal y como señala FRÍAS MARTÍNEZ[761], el artículo 197 *quater* establece una agravación para los supuestos en los que se trata de alguna de las organizaciones citadas en los artículos 570 y siguientes del CP, circunstancia de agravación que como se ha expuesto es de naturaleza específica que incorpora elementos adjetivos. En concreto, contiene un tipo agravado en el que la acción es llevada a cabo en el seno de una organización o grupo criminal en relación con todas las conductas previstas en el Capítulo, entre las que se encuentra el *hacking*.

Como hemos visto, el nuevo precepto encuentra su precedente en el anterior artículo 197.8, introducido por la LO 5/2010, que a su vez tiene su fundamento en los instrumentos internacionales que han pasado a formar parte del ordenamiento jurídico español. Como más relevantes se pueden citar:

(i) la Convención de las Naciones Unidas contra la Delincuencia Organizada Transnacional, hecho en Nueva York el 15 de noviembre de 2000, cuya Asamblea General se declaraba en la

760 VALLE LÓPEZ, M.V., "Los delitos de descubrimiento y revelación de secretos en el Código Penal de 2015: artículos 197, 197 *bis*, 197 *ter*, 197 *quáter*, 197 *quinquies* y 198", en *Revista Penal*, nº 39, ed. Tirant Lo Blanch, Valencia, 2017, p. 196.

761 FRÍAS MARTÍNEZ, E., "Delitos contra la intimidad ...", *cit*., nota 529, p. 370.

Resolución 55/25 de 15 de noviembre de 2000[762], "*Profundamente preocupada por las adversas repercusiones económicas y sociales derivadas de las actividades de la delincuencia organizada y convencida de la necesidad urgente de fortalecer la cooperación para prevenir y combatir más eficazmente esas actividades en los planos nacional, regional e internacional, Observando con profunda preocupación los crecientes vínculos entre la delincuencia organizada transnacional y los delitos de terrorismo y teniendo presente la Carta de las Naciones Unidas y las resoluciones pertinentes de la Asamblea General, Resuelta a impedir que las personas involucradas en la delincuencia organizada transnacional hallen refugio propugnando que se las enjuicie dondequiera que cometan tales delitos y fomentando la cooperación a nivel internacional*" y, en consecuencia, establecía en el artículo 1 de la Convención "*el propósito de promover la cooperación para prevenir y combatir más eficazmente la delincuencia organizada transnacional*";

(ii) la DM 2005/222/JAI, dando así cumplimiento a lo ordenado en su artículo 7.1, donde se dispone que "*Cada Estado miembro adoptará las medidas necesarias para garantizar que las infracciones mencionadas en los artículos 2, apartado 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*

[762] Resolución disponible en http://www.cinu.mx/minisitio/Trafico_migrantes/Conv_Delincuencia_Org.pdf, consultado el 22 de octubre de 2016.

*98/733/JAI, con independencia del nivel de sanción mencionado en dicha Acción Común*", de esta forma, como indica GONZÁLEZ CUSSAC[763], aunque el precepto sólo limitaba la aplicación a los supuestos de acceso ilícito, el legislador español ha optado por extender la aplicación de la agravante a todo el Capítulo. Esta DM fundamenta la reforma relativa a las organizaciones criminales en sus considerandos 2 y 5, donde se constatan los ataques a sistemas de información por medio de delincuencia organizada y la inquietud por los posibles ataques contra sistemas de información básicos para los Estados miembros, lo que supone un riesgo para una sociedad de la información segura y el espacio de libertad, seguridad y justicia, exigiendo la reacción comunitaria. Por ello, se dice que es necesaria la aproximación de las legislaciones penales de los Estados miembros, por cuanto sus divergencias pueden dificultar la lucha contra la delincuencia organizada y complicar la cooperación policial y judicial en los ataques contra los sistemas de información, que frecuentemente tienen carácter transfronterizo atendida la naturaleza transnacional de los sistemas de información: "*(2) 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*

[763] GONZÁLEZ CUSSAC, J. L., "Delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio", en GONZÁLEZ CUSSAC, J. L. (Coord.), y VVAA. *Derecho penal. Parte especial*, ed. Tirant Lo Blanch, Valencia, 2016, p. 288.

*Estados miembros. 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*. (…) *(5) La distancia y las divergencias significativas que existen entre las legislaciones de los Estados miembros en este ámbito pueden dificultar la lucha contra la delincuencia organizada y el terrorismo y pueden complicar la cooperación eficaz de los servicios de policía y las administraciones de justicia en materia de ataques contra los sistemas de información. La naturaleza transnacional y transfronteriza de los modernos sistemas de información significa que los ataques suelen revestir un carácter transfronterizo, lo que plantea la necesidad urgente de proseguir la aproximación de las legislaciones penales en este ámbito*"; y

(iii) la Directiva 2013/40/UE, que declara en su Considerando 13 que "*Es conveniente establecer sanciones más severas cuando un ataque contra un sistema de información se comete en el contexto de una organización delictiva, tal como se define en la Decisión marco 2008/841/JAI del Consejo, de 24 de octubre de 2008, relativa a la lucha contra la delincuencia organizada, o cuando el ciberataque se realiza a gran escala y afecta a un número importante de sistemas de información, en particular cuando el ata que tiene por objeto crear una red infectada o si el ciberataque causa un daño grave, incluido cuando se lleva a cabo a través de una red infectada. Conviene también establecer sanciones más severas cuando el ataque se lleva a cabo contra una infraestructura crítica de los Estados miembros o de*

*la Unión*". Si bien la Directiva sólo se refiere a la aplicación de la agravante a los supuestos de interferencia ilegal en los sistemas de información o en los datos, no mencionando su aplicación a los casos de acceso ilegal a los sistemas de información previstos en su artículo 3[764], el legislador español ha optado por extenderla también a estos supuestos.

Por su parte, la LO 5/2010 justificaba la reforma en materia de delincuencia organizada en el apartado XXVIII de su Preámbulo, refiriéndose a la incapacidad del delito de asociación ilícita vigente para dar respuesta a los distintos supuestos de delincuencia informática, tal y como se había puesto de manifiesto por las distintas resoluciones judiciales. En concreto, el citado apartado establece:

"*el fenómeno de la criminalidad organizada atenta directamente contra la base misma de la democracia, puesto que dichas organizaciones, aparte de multiplicar cuantitativamente la potencialidad lesiva de las distintas conductas delictivas llevadas a cabo en su seno o a través de ellas, se caracterizan en el aspecto cualitativo por generar procedimientos e instrumentos complejos específicamente dirigidos a asegurar la impunidad de sus actividades y de sus miembros, y a la ocultación de sus recursos y de los*

[764] Así, el artículo 9.4 de la Directiva 2013/40/UE establece que "*Los Estados miembros adoptarán las medidas necesarias para garantizar que las infracciones mencionadas en los artícu los 4 y 5 se castiguen con una sanción máxima de privación de libertad de al menos cinco años cuando: a) se cometan en el contexto de una organización delictiva con arreglo a la Decisión marco 2008/841/JAI*".

*rendimientos de aquéllas, en lo posible dentro de una falsa apariencia de conformidad con la ley, alterando a tal fin el normal funcionamiento de los mercados y de las instituciones, corrompiendo la naturaleza de los negocios jurídicos, e incluso afectando a la gestión y a la capacidad de acción de los órganos del Estado*"[765].

Así pues, la reforma de la LO 5/2010, además de introducir el artículo 197.8, opta por ubicar la criminalidad organizada de forma sistemática entre los delitos contra el orden público, Título XXII del Libro II, justificando esta regulación en que estas organizaciones incrementan las posibilidades de agresión con los delitos cometidos en ellas o a través de ellas, generan medios e instrumentos complejos para su impunidad y ocultan lo obtenido bajo la apariencia de legalidad, con lo cual se altera el funcionamiento del mercado e instituciones. En este sentido la STS de 10 de diciembre de 2004[766], en relación con un sujeto que distribuía en Internet material pornográfico donde se utilizaba a menores de edad, había considerado anteriormente que "*cuando de conductas delictivas cometidas por varios partícipes a través de redes informáticas, como INTERNET, se trate, el propio instrumento comisivo, la «red», bastará para integrar tanto la utilización de medios idóneos para configurar la actuación coordinada propia de la organización delictiva, como para alcanzar*

[765] Apartado XXVIII del Preámbulo de la LO 5/2010, disponible en http://www.boe.es/boe/dias/2010/06/23/pdfs/BOE-A-2010-9953.pdf, consultado el 9 de abril de 2017.

[766] STS, Sala Segunda, de 10 de diciembre de 2004, nº 1444/2004, recurso 2385/2003, Pte. Excmo. Sr. D. José Manuel Maza Martín (RJ\2005\879), FJ 3º.

*la finalidad pretendida, a la que ya antes aludíamos, de una mayor facilidad de comisión del delito y capacidad de lesión del bien jurídico protegido, añadiendo especiales dificultades tanto a la prevención como para la persecución del ilícito*" y en este caso, el hecho de que el sujeto actuara en colaboración con otros miembros del grupo de proveedores y consumidores del material prohibido, con una atribución de funciones, como era que aportara fotografías por él elaboradas a un depósito centralizado en una web, "*posibilitaba también el acceso de terceros a esa oferta, como antes decíamos, ampliando la agresión al derecho a la indemnidad sexual de las víctimas de la infracción que es, en definitiva, la razón de ser esencial y el fundamento de la previsión legal agravatoria de la conducta*".

Por tanto, atendido el citado fundamento que se ubica legal y jurisprudencialmente en el incremento de la potencialidad lesiva de los delitos cuando se cometen por estas organizaciones, con medios complejos para su impunidad, la finalidad pretendida de lograr una mayor facilidad para la comisión del delito y para lesionar el bien jurídico protegido, así como las dificultades para su prevención y su persecución y la ampliación de la agresión al bien jurídico, parece correcto considerar que la agravante tiene una naturaleza mixta, objetiva y subjetiva, siguiendo el criterio de ANTÓN ONECA. Así, este autor[767] catalogaba como agravantes mixtas las relativas a los supuestos que denominaba "codelincuencia con armas", que eran los

[767] ANTÓN ONECA, J., *Derecho Penal ...*, *cit*., nota 443, pp. 385, 409 y 412.

de auxilio de gente armada o de personas que aseguren o proporcionen impunidad y la cuadrilla en el Código Penal de 1944. La asociación en estos casos se entendía que estaba entre los delitos más graves, siendo los delincuentes más temibles quienes se asociaban con mayor facilidad y, además, la reunión de varios delincuentes daba lugar a un resultado de mayor intensidad criminal que la suma de los esfuerzos y actividades diversas de cada uno de ellos individualmente considerados, evidenciándose el carácter mixto de estas agravantes que, como hemos visto, serían el precedente lejano de las actuales organizaciones criminales. En consecuencia, en aplicación del artículo 65 CP, por su naturaleza personal la agravante no sólo agravará la responsabilidad de aquéllos en quienes concurra, sino que también atendida la ejecución material del hecho y los medios empleados para realizarla, también va a agravar la responsabilidad de los que tengan conocimiento de ellas en el momento de la acción o de su cooperación para el delito.

Por último, algunos autores como ANARTE BORRALLO y DOVAL PAIS habían sido críticos con esta agravante, por cuanto entendían que esta posibilidad de superagravación, con imposición de pena superior en grado, podía llevar a penas privativas de libertad completamente desproporcionadas atendido el bien jurídico protegido en este ámbito y la aplicación de la agravante a todo el artículo 197, por lo que el criterio político-criminal resultaba muy dudoso, proponiendo su aplicación cautelosa en los casos de acumulación de agravantes, ajustándose a los criterios de incompatibilidad o

inherencia, como en los casos en que existe ánimo de lucro y organización criminal[768].

En este sentido conviene tener en cuenta que aunque el legislador español había dado cumplimiento al mandato del artículo 7.1 de la DM 2005/222/JAI con el artículo 197.8 introducido por la LO 5/2010, también había excedido los límites fijados por esta norma, que prevé "*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*", por cuanto el artículo 197.8 se refería a la totalidad del anterior artículo 197, dando cabida a la pena superior en grado de conductas que conllevaban *per se*, penas de hasta siete años de prisión. Así, p.ej. en el caso de la conducta del anterior artículo 197.7, actual artículo 197.6[769]. De igual forma, el nuevo artículo 197 *quater* se refiere ahora a cualquiera de los hechos previstos en su Capítulo, excediendo de nuevo los límites de la DM, obligando a una interpretación ajustada a los citados criterios de incompatibilidad e inherencia a efectos de evitar penas a todas luces desproporcionadas y fuera del marco fijado por la normativa europea atendidos los citados fundamentos de la agravante. En cualquier caso, tras la reforma de la

---

768 ANARTE BORRALLO, E. y DOVAL PAIS, A., "Delitos contra la intimidad ...", *cit*., nota 166, p. 460. ANARTE BORRALLO, E. y DOVAL PAIS, A., "Delitos contra la intimidad ...", *cit*., nota 380, p. 538.

769 Tanto el anterior artículo 197.7 como el nuevo 197.6 establecen: "*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*".

LO 1/2015 y la tipificación del *hacking* en un artículo propio, ya no resultan aplicables las agravantes del artículo 197 al artículo 197 *bis* evitando así el problema de la superagravación en estos casos. Siendo que no son el objeto de esta obra las restantes conductas que no se refieren al *hacking*, resta concluir que la agravante del artículo 197 *quater* afectará a este delito aumentando en un grado la pena prevista en el artículo 197 *bis* 1, es decir, que conforme al artículo 70.1.1ª CP, en estos supuestos la pena a imponer será la de prisión de 2 a 3 años, o bien, si se trata de favorecer estas conductas conforme al artículo 197 *ter*, la pena será de prisión de 2 a 3 años o de multa de 18 a 27 meses.

### *2.2 La conducta del artículo 197 quater.*

El tipo agravado del artículo 197.8 se presentaba como una de las novedades introducidas con la LO 5/2010 aplicable a todos los supuestos del artículo 197 y que, tras la reforma de la LO 1/2015, con el nuevo artículo 197 *quater* se extiende a todas las conductas previstas en el Capítulo I del Título X del Libro II (*"Si los hechos descritos en este Capítulo se hubieran cometido en el seno de una organización o grupo criminal, se aplicarán respectivamente las penas superiores en grado"*).

A estos efectos tenemos que partir del concepto de organización o grupo criminal, por cuanto la conducta de *hacking* deberá llevarse a cabo en su seno para aplicar la agravante.

La citada STS de 10 de diciembre de 2004[770], con relación a un sujeto que distribuía en Internet material pornográfico donde se utilizaba a menores de edad, después de partir de *"la literalidad del término «organización» empleado por el Legislador que, según el DRALE, significa en nuestra lengua: «Asociación de personas regulada por un conjunto de normas en función de determinados fines»"*, consideraba necesarios *"una serie de requisitos para su aplicación como circunstancia específica de agravación pueden extraerse de la doctrina expuesta, a saber: a) (...) actuación conjunta de una pluralidad de personas, relacionadas entre sí, con reparto de funciones y una base estructurada y jerarquizada, (...) en la que participa continuadamente y no con una mera colaboración ocasional. b) (...) vocación de continuidad, (...) bastando la simple asociación temporal, pero siempre que se trate de algo más que la mera ejecución de una concreta operación delictiva. c) (...) la comisión de los ilícitos pueda subsistir y ser independiente de la actuación individual (...) verdadera «empresa criminal». d) que se cuente con el empleo de medios materiales idóneos (...). e) que todo ello tienda a propiciar una mayor facilidad de comisión del delito y capacidad de lesión del bien jurídico protegido, ofreciendo, además, especiales dificultades tanto a la prevención como para la persecución del ilícito"* y, por último, matizaba el elemento de los medios idóneos:

[770] STS, Sala Segunda, de 10 de diciembre de 2004, *vid*., nota 766, FD 3º.

*"cuando de conductas delictivas cometidas por varios partícipes a través de redes informáticas, como INTERNET, se trate, el propio instrumento comisivo, la «red», bastará para integrar tanto la utilización de medios idóneos para configurar la actuación coordinada propia de la organización delictiva, como para alcanzar la finalidad pretendida, a la que ya antes aludíamos, de una mayor facilidad de comisión del delito y capacidad de lesión del bien jurídico protegido, añadiendo especiales dificultades tanto a la prevención como para la persecución del ilícito".*

Sin embargo, posteriormente, la STS de 20 de septiembre de 2006[771], enjuiciando el caso de un sujeto que se había incorporado a una de las citadas comunidades de Internet, para lo cual debía aportar a la misma fotos de contenido pornográfico y con menores de edad, concluía absolviéndole del delito de corrupción de menores con pertenencia a organización con el siguiente argumento:

"*9. Si queremos manejar el derecho penal con rigor y no con interpretaciones extensivas, tenemos que ajustarnos a los cánones establecidos por la criminología internacional, por los foros de lucha contra la criminalidad organizada y a los parámetros marcados por nuestra jurisprudencia sin aplicaciones extensivas y desmesuradas. El legislador, con vaguedad e imprecisiones, define la organización como un conjunto de tres a más malhechores y les exige una mínima*

[771] STS, Sala Segunda, de 20 de septiembre de 2006, nº 913/2006, recurso 1854/2005, Pte. Excmo. Sr. D. José Antonio Martín Pallín (RJ\2006\6401), FD 1º.

*estructura y coordinación. Esto supone que el concepto de organización lleva implícito un pacto previo en el que se diseñen los modos o formas de actuación, la estructura jerárquica, el reparto de papeles y la continua o frecuente comunicación entre sus componentes. Atribuir todas estas condiciones a una persona que excitada por sus inclinaciones sexuales, actuado en la intimidad de su domicilio, se incorpora a la red y facilita o participa en lo que, en términos internautas se denomina «Chat», me parece una desmesura difícilmente aceptable por el derecho penal. 10. La organización guarda ciertas similitudes con la asociación ilícita. Las acciones ejecutivas imputables a una persona a la que se la adjudica la condición de miembro de una asociación pasa por un cierto dominio del hecho, caso que no concurre en el consumo y aportación de imágenes de origen desconocido a la red de pornografía infantil. Los autores de hechos como el que estamos examinando casi siempre actuarán en función de sus instintos sexuales y nunca por medio de órdenes, instrucciones o cualquier otra tarea previamente convenida*".

Por tanto, con esta STS se consideraba necesario para la existencia de organización el pacto previo sobre los modos o formas de actuación, estructura, reparto de funciones y la frecuente comunicación entre sus miembros, lo que en un sentido restrictivo implicaba excluir a la persona que excitada sexualmente accedía desde su domicilio incorporándose a la red, participando en un chat, concluyendo con las similitudes entre la organización criminal y la

asociación ilícita, de tal manera que se exige para ser miembro tener un cierto dominio del hecho, lo que no ocurría en el consumo y aportación de imágenes a la red, siendo además que los sujetos actuarán normalmente por sus instintos y no por órdenes o tareas acordadas previamente.

Por su parte, el legislador ha simplificado los requisitos y define en el artículo 570 *bis* como "*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*". Por tanto, se mantiene la definición introducida por la LO 5/2010 en el anterior artículo 570 *bis*, si bien tras la reforma de la LO 1/2015, que ha conllevado la eliminación de las faltas, también se ha suprimido en este nuevo artículo la anterior referencia a que "*así como de llevar a cabo la perpetración reiterada de faltas*".

De esta forma, con la LO 5/2010 el legislador español adaptaba la previsión del artículo 7 de la DM 2005/222/JAI, que se remitía al concepto de organización criminal contenido en el artículo 1 de la Acción Común 98/733/JAI[772] y seguía en parte la definición

[772] El artículo 1 de la Acción Común dispone que "*A efecto de la presente Acción común, se entenderá por «organización delictiva» una asociación estructurada de más de dos personas, establecida durante un cierto período de tiempo, y que actúe de manera concertada con el fin de cometer delitos sancionables con una pena privativa de libertad o una medida de seguridad privativa de libertad de un máximo de al menos cuatro años como mínimo o con una pena aún más severa, con independencia de que esos delitos constituyan un fin en sí mismos o un medio de obtener*

contenida en el artículo 1 la DM 2008/841/JAI, a la que se remitía el artículo 9.4.a) de la Directiva 2013/40/UE, aunque esta Directiva sólo se refería a la agravante para los delitos de interferencia ilegal en los sistemas de información y en los datos y no para el *hacking*. Si bien el artículo 1.1 de la DM 2008/841/JAI[773] establecía la siguiente definición:

"«*organización delictiva»: una asociación estructurada de más de dos personas, establecida durante un cierto período de tiempo y que actúa de manera concertada con el fin de cometer delitos sancionables con una pena privativa de libertad o una medida de seguridad privativa de libertad de un máximo de al menos cuatro años o con una pena aún más severa, con el objetivo de obtener,*

---

*beneficios patrimoniales y, en su caso, de influir de manera indebida en el funcionamiento de la autoridad pública. Los delitos a que se refiere el párrafo primero incluyen los mencionados en el artículo 2 del Convenio Europol y en su anexo y que pueden ser sancionados con una pena al menos equivalente a la mencionada en el párrafo primero*". Por su parte, el artículo 2 del Convenio Europol cita "*los delitos cometidos o que puedan cometerse como actividades de terrorismo que atenten contra la vida, la integridad física y la libertad de las personas, así como contra sus bienes, el tráfico ilícito de estupefacientes, las actividades ilícitas de blanqueo de dinero, el tráfico de material nuclear y radiactivo, las redes de inmigración clandestina, la trata de seres humanos y el tráfico de vehículos robados, así como las formas de delincuencia establecidas en el anexo o las manifestaciones específicas de la misma"* y su Anexo incluye, en su lista de delitos, los "*Delitos contra la propiedad, los bienes públicos y delitos de fraude: (…) Delito informático.*".

[773] DM 2008/841/JAI del Consejo, de 24 de octubre de 2008, relativa a la lucha contra la delincuencia organizada, disponible en http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:300:0042:0045:ES:PDF, consultado el 22 de octubre de 2016.

*directa o indirectamente, un beneficio económico u otro beneficio de orden material".*

Por tanto, para el legislador español son necesarias más de dos personas y la actuación de forma concertada, al igual que en la normativa europea, pero puede ser por tiempo indefinido y todo ello con el fin de cometer delitos.

En cuanto al concepto de grupo criminal, el artículo 570 *ter* establece:

"*a los efectos de este Código se entiende por grupo criminal la unión de más de dos personas que, sin reunir alguna o algunas de las características de la organización criminal definida en el artículo anterior, tenga por finalidad o por objeto la perpetración concertada de delitos*".

En consecuencia, también en este caso con la LO 1/2015 se suprime la referencia del anterior artículo 570 *ter* a las faltas, que en este último caso debía tener por finalidad u objeto "*la comisión concertada y reiterada de faltas*".

Aunque los artículos 570 *bis* y 570 *ter* se refieren respectivamente a organización y grupo criminal, con mayores penas para las conductas encuadradas en el primer caso, en el artículo 197 *quater* el legislador ha equiparado ambas conductas atribuyéndoles iguales consecuencias.

La justificación del legislador para considerar más graves las conductas en el seno de organizaciones criminales que en el caso de

los grupos criminales se encuentra en el apartado XXVIII del Preámbulo de la LO 5/2010[774], argumentando la necesidad de llevar a cabo la comprobación de una estructura más compleja que no tienen los grupos criminales y que supone una amenaza mayor para la seguridad y el orden jurídico.

En este sentido, la STS de 22 de diciembre de 2014[775] recordaba que el elemento distintivo entre organización y grupo se encuentra en el carácter estable y la concertación y coordinación en el reparto de funciones de sus integrantes, lo cual no es necesario en el grupo:

---

774 Respecto a la citada justificación, este apartado dispone que "*Hay que recordar también que la jurisprudencia relativa al delito de asociación ilícita, así como la que ha analizado las ocasionales menciones que el Código Penal vigente hace a las organizaciones criminales (por ejemplo, en materia de tráfico de drogas), requiere la comprobación de una estructura con vocación de permanencia, quedando fuera por tanto otros fenómenos análogos muy extendidos en la sociedad actual, a veces extremadamente peligrosos o violentos, que no reúnen esos requisitos estructurales. La necesidad de responder a esta realidad conduce a la definición, en paralelo con las organizaciones, de los que esta Ley denomina grupos criminales, definidos en el nuevo artículo 570 ter precisamente por exclusión, es decir, como formas de concertación criminal que no encajan en el arquetipo de las citadas organizaciones, pero sí aportan un plus de peligrosidad criminal a las acciones de sus componentes. (…) La estructura de las nuevas infracciones responde a un esquema similar en ambos casos, organizaciones y grupos, si bien por un lado las penas son más graves en el caso de las primeras, cuya estructura más compleja responde al deliberado propósito de constituir una amenaza cualitativa y cuantitativamente mayor para la seguridad y orden jurídico*".

775 STS, Sala Segunda, de 22 de diciembre de 2014, nº 877/2014, recurso 10636/2014, Pte. Excmo. Sr. D. Juan Ramón Berdugo y Gómez de la Torre (RJ\2014\6661), FD 3º.

"*ambas precisan la unión o agrupación de mas de dos personas y la finalidad de cometer delitos, pero mientras que la organización criminal requiere, además, el carácter estable o su constitución o funcionamiento por tiempo indefinido, y que de manera concertada y coordinada se repartan las tareas o funciones entre sus miembros con aquella finalidad, el grupo criminal puede apreciarse aunque no concurra ninguno de estos dos requisitos, o cuando concurra solo uno de ellos. Por tanto el grupo criminal requiere solamente la unión de más de dos personas y la finalidad de cometer concertadamente delitos o reiteradamente faltas. La ley permitiría configurar el grupo criminal con esas dos notas, pues la definición legal contempla la posibilidad de que no concurran alguna o algunas de las que caracterizan la organización, que además de las coincidentes, esto es, la unión o agrupación de más de dos personas y la finalidad de cometer de forma concertada delitos o reiteradamente faltas, son solamente dos: la estabilidad y el reparto de tareas -lo que excluye en supuestos de transitoriedad que habrían de incluirse en su caso, en la figura del grupo criminal*". De esta forma, la STS declara que el legislador está *"Reconociendo, por lo tanto, dos niveles de peligro para los bienes jurídicos protegidos, que hacían a las respectivas conductas acreedoras a distinta gravedad en la sanción penal. No debe realizarse, por lo tanto, una interpretación extensa del concepto de organización, ya que conduciría a incluir en el mismo supuestos más propios, por su gravedad, del concepto de grupo criminal, con el riesgo de dejar a éste prácticamente vacío de contenido*".

Por último, establecida la distinción entre organización y grupo criminal, y conforme a lo apuntado en la última Sentencia citada, no debe confundirse esta última con los casos de mera codelincuencia, por cuanto, tal y como señala CUERDA ARNAU, los amplios contornos que abarcan organización y, con carácter residual, el grupo criminal, puede suponer la eliminación de las reglas en materia de participación delictiva[776], lo que en los casos de *hacking* podría dar lugar a reconducir los casos al artículo 197 *quater*. Así, GONZÁLEZ RUS critica la versión extravangante de la criminalidad organizada, que hace posible el castigo de todo lo que pueda relacionarse con ella y además permite castigarlo con extrema dureza[777].

Conforme expone GARCÍA ALBERO, estas organizaciones o grupos no se agotan en la puntual realización de un único hecho delictivo a cuyo servicio se ha constituido el concierto criminal[778]. Además, siguiendo a VELASCO NUÑEZ[779], existen una serie de caracteres o requisitos de carácter nuclear en la agravante de pertenencia a organización/grupo/asociación en los delitos

---

776 CUERDA ARNAU, M. L., "Delitos contra el orden …", *cit*., nota 750, pp. 759 y 760.

777 GONZÁLEZ RUS, J. J., "La criminalidad organizada en el Código Penal Español. Propuestas de reforma", en *Anales de derecho*, nº 30, ed. Universidad de Murcia, Murcia, 2012, p. 17, disponible en http://revistas.um.es/analesderecho/article/view/161841/142081, consultado el 9 de abril de 2017.

778 GARCÍA ALBERO, R., "Delitos contra el orden público", en QUINTERO OLIVARES (Dir.) y VVAA. *Comentarios a la parte especial del Derecho penal*, ed. Aranzadi, Navarra, 2016, p. 2161.

779 VELASCO NUÑEZ, E., "Delitos informáticos ...", *cit*., nota 665, pp. 4 y 5.

informáticos conforme a la jurisprudencia anterior a la LO 5/2010 y que según este autor el legislador hizo suyos: (i) la necesidad de una pluralidad de personas coordinadas entre sí, se conozcan personalmente o no, habiendo decidido el legislador que sean más de dos personas (artículos 570 *bis* y 570 *ter* CP); y (ii) la agravante exige "pertenencia", lo cual supone excluir la colaboración accidental u ocasional, existiendo cierta vocación de continuidad, que se matiza en una "*mínima permanencia para superar la mera codelincuencia*". Estos son los dos caracteres que diferencian la agrupación o asociación de la mera coautoría o coparticipación, denominados por este autor como nucleares, junto a los que se ubicarían los requisitos adjetivos, que no son nucleares pero sí reafirman la agravación: (i) la estructura jerárquica, no necesariamente piramidal, pudiendo ser "estructuras en red" entre personas que no se conocen físicamente pero mantienen un contacto continuado a través de las telecomunicaciones; (ii) el uso de medios especialmente idóneos para conseguir el fin perseguido; (iii) la programación de un proyecto para desarrollar la idea criminal, que puede ser un nexo común entre los asociados; y (iv) "reparto de papeles" y distribución específica de funciones o roles, que se caracterizan por su sustituibilidad, debiendo subsistir la operación criminal con independencia de cada componente individual del grupo, sin que sea necesario que cada uno conozca las misiones de cada uno.

Con posterioridad a este criterio, la citada la STS de 22 de diciembre de 2014 ha establecido que la mera codelincuencia "*se*

*apreciaría, en primer lugar, en aquellos casos en los que la unión o agrupación fuera solo de dos personas*", pero esto no significa que cuando existan más de dos integrantes estaremos necesariamente ante un grupo criminal, sino que en estos casos el Tribunal Supremo se remite a la normativa internacional. En concreto, a la Convención de las Naciones Unidas contra la Delincuencia Organizada Transnacional de 15 de noviembre de 2000, firmada por España en Palermo el 13 de diciembre de 2000[780]:

"*En el artículo 2 de la citada Convención se establecen las siguientes definiciones: en el apartado a) Por "grupo delictivo organizado" [ORGANIZACIÓN] se entenderá un grupo estructurado de tres o más personas que exista durante cierto tiempo y que actúe concertadamente con el propósito de cometer uno o más delitos graves o delitos tipificados con arreglo a la presente Convención con miras a obtener, directa o indirectamente, un beneficio económico u otro beneficio de orden material; y en el apartado c) Por "grupo estructurado" [GRUPO] se entenderá un grupo no formado fortuitamente para la comisión inmediata de un delito y en el que no necesariamente se haya asignado a sus miembros funciones formalmente definidas ni haya continuidad en la condición de miembro o exista una estructura desarrollada".*

[780] El Instrumento de Ratificación de la Convención de las Naciones Unidas contra la Delincuencia Organizada Transnacional, hecho en Nueva York el 15 de noviembre de 2000, publicado en el BOE nº 233, de 29 de septiembre de 2003, disponible en https://www.boe.es/buscar/doc.php?id=BOE-A-2003-18040, consultado el 1 de mayo de 2017.

De esta forma, siendo estas las características del grupo criminal frente a la mera codelincuencia, podemos concluir, como dice la STS de 10 de julio de 2015[781], que "*la codelincuencia se apreciaría en los casos de agrupaciones o uniones de solo dos personas, o cuando estando integradas por más de dos personas, se hubieran formado fortuitamente para la comisión inmediata de un delito*".

Todo ello, recordando la mencionada STS de 22 de diciembre de 2014 que también es posible la existencia de una organización para una operación específica si concurren el delito de decisiones y la organización jerárquica, existiendo una red de reemplazo que asegure el proyecto criminal:

"*No siendo ocioso recordar que es admisible una organización para una operación especifica siempre que concurran los elementos propios de la organización criminal, un delito de decisiones y diversos niveles jerárquicos, con posibilidad de institución de unos a otros mediante una red de reemplazo que asegure de su pervivencia del proyecto criminal, pues esto es lo que dificulta la prevención y persecución de los delitos cometidos por la organización criminal y agrava el daño ocasionado por su actividad, permitiendo hablar de "empresa criminal" (SSTS. 164/2006 de 22.2 (RJ 2006, 4741), 323/2006 de 22.3 (RJ 2006, 4784), 780/2007 de 3.10 (RJ 2008,*

[781] STS, Sala Segunda, de 10 de julio de 2015, nº 454/2015, recurso 10746/2014, Pte. Excmo. Sr. D. Juan Ramón Berdugo y Gómez de la Torre (RJ\2015\6558), FD 8º.

*780), 16/2009 de 27.1, 1119/2009 de 6.11 (RJ 2010, 115) )*".

En consecuencia, aunque se ha destacado la utilidad de la agravante en relación con el *hacking*, por cuanto son numerosas las estafas informáticas a gran escala llevadas a cabo por organizaciones criminales que se valen de *hackers* para acceder a sistemas y obtener la información con la que posteriormente defraudar[782], no se entiende que en el caso del artículo 197 *quater* el legislador haya decidido equiparar las conductas de *hacking* llevadas a cabo en el seno de una organización con las mismas conductas realizadas en un grupo criminal, es decir, la estabilidad de una organización para delinquir con una posible unión transitoria de más de dos personas para llevar a cabo ese acceso, resultando criticable esta equiparación que no existe en los artículos 570 *bis* y 570 *ter* CP y que se aparta del criterio jurisprudencial expuesto, donde se reconocen los dos niveles de peligro para los bienes jurídicos protegidos en función de que se trate de organización o grupo criminal:

"*1º) Para la lucha contra la delincuencia organizada transnacional, caracterizada por su profesionalización, tecnificación e integración en estructuras legales ya sean económicas, sociales e institucionales, para lo cual se diseña como figura específica la Organización criminal, del Art. 570 bis. 2º) Para la pequeña criminalidad organizada de ámbito territorial más limitado y cuyo objetivo es la realización de actividades delictivas de menor entidad,*

[782] MIRÓ LLINARES, F., "Los Delitos Informáticos ...", *cit*., nota 108, p. 155.

*para lo cual se diseña como figura específica el grupo criminal, del Art. 570 ter*", determinando así la distinta gravedad en la sanción.

En la misma línea, el FJ 8º de la STS de 10 de julio de 2015, declara que

"*No debe realizarse, por lo tanto, una interpretación extensa del concepto de organización, ya que conduciría a incluir en el mismo supuestos más propios, por su gravedad, del concepto de grupo criminal, con el riesgo de dejar a este prácticamente vacío de contenido".*

De esta forma, existiendo la diferenciación legal y jurisprudencial y estando justificado el fundamento de la distinta pena en uno y otro caso, el legislador también debería haber explicado la equiparación que en el artículo 197 *quater* realiza entre ambos grupos para imponerles la misma pena.

Podemos concluir con VELASCO NUÑEZ[783] que al quedar absorbidas organización y grupo, aplicándose con independencia de que la actuación del grupo tenga o no permanencia en el tiempo, se producirá la incompatibilidad de añadirla como actuación que acompañe a los supuestos previstos en los artículos 570 *bis* y 570 *ter* CP.

[783] VELASCO NUÑEZ, E., "Delitos informáticos …", *cit*., nota 665, p. 9.

### *2.3 Posición personal.*

La agravante del artículo 197 *quater* está prevista para los supuestos en que las conductas se cometan en el seno de organizaciones o grupos criminales, aplicándose las penas superiores en grado a todas las conductas del capítulo.

En el anterior artículo 197.8 la referencia era únicamente a las conductas del artículo 197, lo que llevaba una agravación desproporcionada: en primer lugar, atendido el bien jurídico protegido, tanto si se considera la intimidad, como si se considera la seguridad o integridad de los sistemas de información, pudiendo llegar a imponerse una pena superior incluso a la prevista en el artículo 138 CP para el homicidio; y en segundo lugar, por el hecho de que la LO 5/2010 ya había introducido un capítulo específico (artículos 570 *bis*, *ter* y *quater*) para reprimir las conductas de las organizaciones o grupos terroristas. Con el actual artículo 197 *quater* la referencia es a todas las conductas del capítulo. No obstante, puesto que ahora el *hacking* tiene su regulación específica en el artículo 197 *bis* 1, ya no tiene lugar la aplicación de la agravante de llevar a cabo la conducta en el seno de una organización o grupo criminal sobre, por ejemplo el *hacking* con ánimo de lucro prevista en el anterior artículo 197.7, que ya no está previsto en relación con la conducta que nos ocupa, por lo que considero que el legislador ha moderado la excesiva represión que se había establecido con la agravante para estas conductas.

En cuanto al fundamento de la agravante, los instrumentos internacionales, el Preámbulo de la LO 5/2010 y la jurisprudencia que los interpreta, donde se reitera: su potencialidad lesiva, incrementada en los delitos cuando se cometen por medio de estas organizaciones o grupos; el empleo de medios complejos para lograr la impunidad; la finalidad dirigida a facilitar la comisión del delito y lesionar el bien jurídico protegido; las dificultades para la prevención y persecución; y la mayor lesión para el bien jurídico, me llevan a la conclusión de que es una agravante mixta, donde concurren elementos objetivos y subjetivos, y con la que se trata de prevenir y mejorar la lucha contra la criminalidad organizada a través de las nuevas tecnologías[784], atendido el incremento en el desvalor de la acción y del resultado[785], fundamentando así el mayor castigo.

Por lo que respecta a la conducta agravada del artículo 197 *quater*, todavía no ha sido objeto de desarrollo jurisprudencial, habiendo sido escasos los pronunciamientos cuando se ha tratado de otras conductas realizadas a través de Internet, especialmente en los supuestos de organizaciones criminales relacionadas con la pornografía infantil. Al respecto, en el punto anterior se ha analizado la STS de 10 diciembre de 2004, donde se mencionaban los requisitos para apreciar la organización criminal y se concluía que el empleo de las redes informáticas, como Internet, es suficiente para integrar la

[784] Así, MIRÓ LLINARES, F., "Los Delitos Informáticos ...", *cit*., nota 108, p. 155.

[785] En este sentido, MORALES PRATS, F., "Delitos contra la intimidad ...", *cit.*, nota 489, p. 480.

utilización de medios idóneos para la actuación coordinada de la organización y el alcance de la finalidad pretendida, consistente en la facilidad de comisión del delito y la capacidad de lesión del bien jurídico protegido, dificultando tanto la prevención como su persecución. Sin embargo, como se ha visto, la STS de 20 de septiembre de 2006 cambia ese criterio y considera que la organización conlleva un pacto previo sobre las formas de actuación, estructura, reparto de funciones y la continua comunicación de sus miembros, lo cual no sucedería en la persona que movida por sus instintos sexuales desde su domicilio se incorpora a la red y participa en un chat. Según esta STS, era necesario un cierto dominio del hecho, como en la asociación ilícita, lo que no sucede con el mero consumo y aportación de imágenes, donde además no concurren órdenes, instrucciones o tareas previamente convenidas.

No obstante el cambio de criterio jurisprudencial juzgando casos de pornografía infantil y la posible integración en organización criminal, entiendo que es más acertado el criterio de la STS de 2004 y con ella pensar que el sujeto que accede desde su domicilio a Internet, a una comunidad que tiene un claro objeto delictivo, como sería en el caso que nos ocupa una comunidad de *hackers*, es decir, el objeto de acceder a otros sistemas informáticos ilícitamente o compartir y recibir información o medios para hacer posible el acceso, lo hace participando de una organización criminal por lo siguientes motivos:

1.- Concurren más de dos personas, en una comunidad o *web* que, por tanto, tiene un carácter estable y un funcionamiento

concertado y coordinado por su creador o creadores y dirigido a la comisión del delito, siendo acorde con la definición de organización criminal del artículo 570 *bis* CP.

Dicho en otras palabras, el sujeto se está valiendo de un medio idóneo para delinquir y existe una actuación coordinada propia de una organización, por cuanto no olvidemos que antes previamente alguien ha creado esa comunidad virtual y ha establecido unas reglas de acceso y un claro objeto criminal, todo ello aceptado por el sujeto que pasa a formar parte de ella con el acceso y aportación de información o medios.

2.- Sabe que accede a un sitio donde es sencilla la comisión del delito y, por tanto, lesionar el bien jurídico protegido, siendo difícil la prevención y persecución del delito. Por tanto, se trataría, empleando los términos del artículo 5.1.a.ii) de la Convención de las Naciones Unidas contra la Delincuencia Organizada Transnacional, de 15 de noviembre de 2000, de una "*conducta de toda persona que, a sabiendas de la finalidad y actividad delictiva general de un grupo delictivo organizado o de su intención de cometer delitos en cuestión, participe activamente en: a. Actividades ilícitas del grupo delictivo organizado; b. Otras actividades del grupo delictivo organizado, a sabiendas de que su participación contribuirá al logro de la finalidad delictiva antes descrita*".

3.- Como se establece en el apartado XXVIII del Preámbulo de la LO 5/2010, "*Las organizaciones y grupos criminales en general no son realmente «asociaciones» que delinquen, sino agrupaciones de*

*naturaleza originaria e intrínsecamente delictiva, carentes en muchos casos de forma o apariencia jurídica alguna"* contraviniendo así la mencionada equiparación que hacía la STS de 2006 entre organización criminal y la asociación ilícita.

Todo ello, salvo que se tratara de un mero acceso del sujeto a la comunidad de forma accidental u ocasional, por cuanto siguiendo a VELASCO NÚÑEZ[786], entiendo necesario una pluralidad de personas coordinadas entre sí y una mínima permanencia para superar la mera codelincuencia, es decir, conforme expone GARCÍA ALBERO, no se agotan en la puntual realización de un único hecho delictivo a cuyo servicio se ha constituido el concierto criminal[787]. Junto a estos dos requisitos esenciales, que se darían en los mencionados supuestos de comunidad o *web* para llevar a cabo el *hacking* o para facilitar la información o medios de acceso, además también concurrirían los denominados elementos adjetivos[788], como son (i) la estructura jerárquica, que vendría dada por los sujetos que se incorporan a ella y, por encima de ellos, por el creador de la comunidad o web que establece las reglas para formar parte de ella y fija el objeto delictivo, de tal forma que podría cerrarla en el caso de que sus reglas no fuesen

---

786 VELASCO NUÑEZ, E., "Delitos informáticos ...", *cit*., nota 665, p. 4 y 5.

787 GARCÍA ALBERO, R., "Delitos contra el orden público ...", *cit*., nota 778, p. 2161.

788 Sobre la denominación de elementos adjetivos en las organizaciones y grupos criminales, VELASCO NUÑEZ, E., "Delitos informáticos ...", *cit*., nota 665, p. 4 y 5.

respetadas o el objeto fuese inicialmente lícito pero se hubiera tornado ilícito contra lo que se pretendía; (ii) los medios especialmente idóneos para el fin perseguido, como son las nuevas tecnologías a través de Internet o una estructura de redes; (iii) la existencia de un proyecto para desarrollar la idea criminal, como son las reglas establecidas por el creador o por los integrantes de la organización para llevar a cabo el acceso ilícito a uno o varios sistemas de información; y (iv) la fungibilidad o sustituibilidad de los integrantes, por cuanto existiendo la comunidad o web o punto de encuentro conforme a las reglas establecidas por su creador, cualquiera de sus miembros aportará y recibirá información o medios para acceder ilícitamente a uno o varios sistemas informáticos, sin que sea necesario que conozcan las funciones o roles asumidos por los otros miembros de la organización.

Por último, a pesar de que ya no esté previsto para el supuesto de *hacking* la aplicación acumulativa de la agravante con las previstas en el artículo 197, es criticable la equiparación de penas en el artículo 197 *quater* cuando el delito es cometido en el seno de una organización o de un grupo criminal, atendida la distinción conceptual y penológica en los artículos 570 *bis* y 570 *ter* y el fundamento que el propio legislador establece en el Preámbulo de la LO 5/2010 para las mayores penas en el caso de organizaciones criminales. Considero que de forma coherente se debería haber eliminado el artículo 197 *quater*, llevando estas conductas a los artículos 570 *bis* y 570 *ter*, o bien se debería haber mantenido el artículo 197 *quater* con una diferenciación

de penas en función de que la conducta se lleve a cabo en el seno de una organización o grupo criminal. Este planteamiento me parece el más acorde con la clara distinción legal y jurisprudencial entre los dos niveles de riesgo para los bienes jurídicos protegidos según se trate por una parte de organización o, por otra, de grupo criminal. Tal y como se ha expuesto en el punto anterior, la jurisprudencia ha advertido de la inconveniencia de realizar una interpretación extensiva de la idea de organización criminal, por cuanto ello llevaría a incluir supuestos que por su gravedad deberían reconducirse al concepto de grupo criminal y, a su vez, se estaría dejando estos supuestos vacíos de contenido. Por todo ello, el legislador debería haber fundamentado su criterio de equiparar las organizaciones y los grupos criminales cuando llevan a cabo el delito de *hacking* que nos ocupa. No haberlo hecho lleva a la conclusión, por una parte, de que cuando se trata del acceso o mantenimiento a todo o parte de un sistema de información, es irrelevante si se accede o se permanece como miembro de una organización o un grupo criminal, por cuanto la sanción va a ser la misma a pesar de la distinción prevista en la normativa internacional, en los artículos 570 *bis* y 570 *ter* CP y en la jurisprudencia que los ha desarrollado y, por otra parte, a la incompatibilidad del artículo 197 *quater* con la aplicación de los citados artículos.

### *3. EL TIPO AGRAVADO DEL ARTÍCULO 198.*

Ya se ha hecho referencia anteriormente a las relaciones concursales del intrusismo informático con otros delitos en general[789]. Por ello, antes de analizar en particular el *hacking* en relación con la conducta del artículo 198 CP, conviene precisar que este precepto guarda similitud con otras disposiciones del Código, como los artículos 414, 415 o 536 CP.

Así, en el caso del artículo 414 CP, se castiga en su primer apartado "*A la autoridad o funcionario público que, por razón de su cargo, tenga encomendada la custodia de documentos respecto de los que la autoridad competente haya restringido el acceso, y que a sabiendas destruya o inutilice los medios puestos para impedir ese acceso o consienta su destrucción o inutilización, incurrirá en la pena de prisión de seis meses a un año o multa de seis a veinticuatro meses y, en cualquier caso, inhabilitación especial para empleo o cargo público por tiempo de uno a tres años"*, mientras que en su segundo apartado se establece que "*El particular que destruyere o inutilizare los medios a que se refiere el apartado anterior, será castigado con la pena de multa de seis a dieciocho meses".*

Por tanto, en estos casos se exige que se trate del acceso a documentos y no meramente a un sistema informático que pudiera contenerlos, por lo que su especialidad y mayor gravedad determina

789 *Vid., supra* Capítulo IV, subepígrafe 5.3.

que se deberá resolver a su favor un hipotético concurso de normas con las conductas de facilitar el acceso a un sistema del artículo 197 *bis* 1 CP.

Por su parte, el artículo 415 CP dispone:

"*La autoridad o funcionario público no comprendido en el artículo anterior que, a sabiendas y sin la debida autorización, accediere o permitiere acceder a documentos secretos cuya custodia le esté confiada por razón de su cargo, incurrirá en la pena de multa de seis a doce meses, e inhabilitación especial para empleo o cargo público por tiempo de uno a tres años*".

Se puede plantear el caso de que los documentos secretos se encuentren en un sistema informático. En este supuesto, siguiendo el mismo criterio de ANARTE BORRALLO y DOVAL PAÍS con ocasión del anterior artículo 197.3 en relación con el artículo 197.2 CP, podemos llegar a la conclusión expuesta en el caso anterior, es decir, se aplicaría el criterio de la consunción del delito cuyo umbral típico se ubica más lejos de la afección al bien jurídico protegido[790] y por tanto, en este caso, estando más lejos el artículo 198 CP, el concurso de normas se resolvería a favor del artículo 415 CP. En este sentido, ROMEO CASABONA también mantenía el criterio de la especialidad para resolver el concurso de normas entre las conductas

[790] ANARTE BORRALLO, E. y DOVAL PAIS, A., "Límites de la ley penal ...", *cit*., nota 24, p. 31.

del artículo 415 y 198, a la vista de que el deber infringido por el funcionario es más específico[791].

Por su parte, el artículo 536 CP establece en su primer párrafo:

"*La autoridad, funcionario público o agente de éstos que, mediando causa por delito, interceptare las telecomunicaciones o utilizare artificios técnicos de escuchas, transmisión, grabación o reproducción del sonido, de la imagen o de cualquier otra señal de comunicación, con violación de las garantías constitucionales o legales, incurrirá en la pena de inhabilitación especial para empleo o cargo público de dos a seis años*".

Sin embargo, el artículo 198 CP tiene la peculiaridad de que, en relación con las conductas de *hacking* que nos ocupan, además de requerir un acceso al sistema informático en los términos que se vienen exponiendo, exigiría que la autoridad o funcionario público actuase "*fuera de los casos permitidos por la Ley*", "*sin mediar causa legal por delito*" y "*prevaliéndose de su cargo*"[792]. De esta forma,

---

791 ROMEO CASABONA, C. M., *Los delitos de descubrimiento y revelación de secretos. Especial consideración a su comisión en conexión con las nuevas tecnologías de la información y de la comunicación*, ed. Tirant Lo Blanch, Valencia, 2005, epígrafe VI, página 6.

792 En este sentido, la STS, Sala Segunda, de 3 de febrero de 2009, nº 123/2009, recurso 1462/2007, Pte. Excmo. Sr. D. Luciano Varela Castro (EDJ 2009/50757), declaraba en su FD Único la aplicación del artículo 198 del CP a uno de los acusados que había accedido a datos reservados de carácter personal, en concreto un acceso a un registro que contenía entre otros datos los antecedentes policiales del padre y hermano de la denunciante, pero para obtener datos de un vehículo, condenando al acusado por un delito de revelación de secretos del artículo 197.2, conforme al artículo 198,

como señala MORALES PRATS, el delito del artículo 198 CP se ocupa de incluir conductas en el ámbito de las relaciones de la Administración-ciudadano u otras relaciones Estado-ciudadano, cuando no medie la investigación de una causa penal[793]. A todo ello se añadiría la circunstancia indicada por GONZÁLEZ CUSSAC de falta de conducta pluriofensiva en el artículo 198 CP, por no tutelarse el correcto ejercicio de la función pública, que podrá ser en alguna ocasión objeto de lesión, pero no siempre[794], pudiendo plantearse según este autor y CARBONELL MATEU un concurso de leyes entre los supuestos de los artículos 198 y 536 CP[795], tal y como hemos visto en los casos anteriores.

No obstante, otros autores como ROMEO CASABONA han mantenido que en realidad el artículo 536 configura un supuesto de tipicidad en principio bien delimitado en relación con los elemento típicos previstos en el artículo 198, por lo que en puridad no parece que pueda plantearse un concurso de normas[796]. De esta forma,

---

por "*ser el acusado funcionario y haber accedido prevaliéndose de su condición de tal sin que mediara supuesto que legitimase ese acceso*".

793 MORALES PRATS, F., "Delitos contra la intimidad ...", *cit.*, nota 489, p. 482.

794 GONZÁLEZ CUSSAC, J. L., "Delitos contra la intimidad ...", *cit*., nota 763, p. 289.

795 CARBONELL MATEU, J. C., y GONZÁLEZ CUSSAC, J. L., "Artículo 198", en VIVES ANTÓN, T. (Coord.) y VVAA, *Comentarios al Código Penal de 1995*, ed. Tirant Lo Blanch, Valencia, 1996 (libro electrónico sin numeración de páginas).

796 ROMEO CASABONA, C. M., *Los delitos de descubrimiento ...*, *cit*., nota 791, epígrafe VI, página 6.

podrían ocurrir situaciones tales como que la autoridad o funcionario público intercepte las telecomunicaciones o utilice alguno de los artificios citados en el artículo 536 CP para de esta forma acceder al sistema informático, supuestos en los que habría que analizar la concurrencia de las circunstancias que integran el tipo del artículo 536 o del 198 CP para resolver la aplicación de uno u otro precepto.

Por tanto, a continuación se expone una aproximación a los citados elementos en relación con el *hacking*, teniendo presente que, tal y como se ha expuesto en la introducción, en tanto no se modifique la redacción del artículo, tendrá una difícil aplicación práctica para el intrusismo informático.

### *3.1 El concepto de "autoridad o funcionario público".*

Considerando con ORTS BERENGUER y GONZÁLEZ CUSSAC como delitos especiales impropios aquellos en los que las características del sujeto activo determinan un castigo diferente[797], el delito previsto en el artículo 198 CP se configura como uno de los supuestos encuadrables en esa categoría.

Este es el criterio mantenido también por la jurisprudencia, al mencionar que el precepto contiene un delito especial impropio o

[797] ORTS BERENGUER, E. y GONZÁLEZ CUSSAC, J. L., *Compendio de Derecho penal …*, *cit*., nota 465, p. 243.

alternativa típica agravada por las características del autor[798], que es la autoridad o el funcionario público. Esta naturaleza resultaría de que el delito de *hacking* puede ser cometido por cualquiera, siendo por tanto común, pero se agravaría en el artículo 198 CP para el caso de que sea cometido por autoridad o funcionario público. La consecuencia, siguiendo a MOLINA FERNÁNDEZ[799], es que, si intervienen varios sujetos, cada uno deberá responder conforme a su hecho y culpabilidad, es decir, conforme al artículo 65 CP. Esto significa que la autoridad o funcionario público responderá conforme al artículo 198 CP y quien no tenga esa condición quedará sujeto al artículo 197 *bis* 1 CP.

Por tanto, como señalan ANARTE BORRALLO y DOVAL PAIS, se trata de una agravante por razón del sujeto que realiza la conducta, con un doble fundamento: en primer lugar, la mayor facilidad para cometer el delito y, en segundo lugar, por la vulneración de su deber de corrección en el cumplimiento de su cargo. Todo ello con el motivo político criminal añadido de la prevención general[800].

---

798 Esta es la definición también de la STS, Sala Segunda, de 11 de junio de 2004, nº 725/2004, recurso 471/2003, Pte. Excmo. Sr. D. Enrique Bacigalupo Zapater (EDJ 2004/82679), FD 10º: "*el art. 198 CP EDL 1995/16398 prevé -como delito especial impropio, es decir, como alternativa típica agravada por las características del autor*".

799 MOLINA FERNÁNDEZ, F., "Autoría y participación delictiva", en MOLINA FERNÁNDEZ, F. (Coord.) y VVAA, *Memento práctico penal 2017*, ed. Francis Lefebvre, Madrid, 2016, p. 347.

800 ANARTE BORRALLO, E. y DOVAL PAIS, A., "Delitos contra la intimidad ...", *cit*., nota 166, p. 459.

De esta forma con la incorporación del artículo 198 en el CP y relacionado con los supuestos de acceso ilícito a todo o parte de un sistema de información, se pondría fin al tratamiento privilegiado para las autoridades o funcionarios públicos que llevaban a cabo injerencias ilegítimas en los derechos y libertades de los ciudadanos, recibiendo ahora un tratamiento agravado respecto al correlativo delito de *hacking* y abandonando de esta forma un incomprensible tratamiento atenuado para estos sujetos[801].

Por tanto, para que tenga lugar la aplicación del artículo 198 en relación con las conductas de *hacking*, en primer lugar, es necesario que sea llevada a cabo por autoridad o funcionario público. Como es sabido, existe un concepto normativo que está incluido en el artículo 24 CP, donde se define como autoridad "*al que por sí solo o como miembro de alguna corporación, tribunal u órgano colegiado tenga mando o ejerza jurisdicción propia. En todo caso, tendrán la consideración de autoridad los miembros del Congreso de los Diputados, del Senado, de las Asambleas Legislativas de las Comunidades Autónomas y del Parlamento Europeo. Se reputará*

[801] Como se dice en la Exposición de Motivos del CP: "*en consonancia con el objetivo de tutela y respeto a los derechos fundamentales, se ha eliminado el régimen de privilegio de que hasta ahora han venido gozando las injerencias ilegítimas de los funcionarios públicos en el ámbito de los derechos y libertades de los ciudadanos. Por tanto, se propone que las detenciones, entradas y registros en el domicilio llevadas a cabo por autoridad o funcionario fuera de los casos permitidos por la Ley, sean tratadas como formas agravadas de los correspondientes delitos comunes, y no como hasta ahora lo han venido siendo, esto es, como delitos especiales incomprensible e injustificadamente atenuados"*.

*también autoridad a los funcionarios del Ministerio Fiscal*", mientras que funcionario público es "*todo el que por disposición inmediata de la Ley o por elección o por nombramiento de autoridad competente participe en el ejercicio de funciones públicas*".

La jurisprudencia ha reiterado que esta definición de funcionario es privativa del Derecho penal, sin que pueda determinarse por criterios del Derecho administrativo o social[802].

Se han considerado funcionarios a efectos de las conductas del artículo 198, entre otros y en relación con las conductas de accesos a

---

802 En este sentido, la STS, Sala Segunda, de 11 de octubre de 1993, nº 2208/1993, recurso 3286/1989, Pte. Excmo. Sr. D. Justo Carrero Ramos (RJ 1993\7705), FD 1º, consideraba funcionario público al "*ordenanza de un organismo oficial de la Administración autonómica*", conforme a la definición del anterior artículo 119 CP, "*El art. 119 del Código Penal da un concepto de funcionario público propio y privativo de este campo jurídico. Y que es el que rige a todos los efectos de aplicación de sus normas y, por lo tanto, del art. 403 del mismo. No se trata, pues, de una norma en blanco que pueda remitir la definición a otras disposiciones, del Derecho Administrativo o Laboral, con las que puede no concordar*".

Por el contrario, siguiendo el mismo criterio, la STS, Sala Segunda, de 10 de diciembre de 2007, nº 1122/2007, recurso 576/2007, Pte. Excmo. Sr. D. Francisco García Pérez (RJ 2007\9120), FD 2º y 3º, consideraba que el acusado no podía ser considerado funcionario público por ser "*trabajador laboral, mecánico oficial de primera, en la empresa Applus Iteuve, concesionaria de la Generalitat de Catalunya para la inspección técnica de vehículos*", argumentando que "*La doctrina de esta Sala ha dejado claro que el concepto de funcionario público a que se refiere el art. 24 es privativo del Derecho Penal, de manera que no puede ser remitida la consideración de tal carácter a criterios del Derecho Administrativo o del social; véanse las sentencias de 4/12/2001 (RJ 2002, 817) y, para el anterior art. 119, la de 11/10/1993 (RJ 1993, 7705). Lo que, a su vez, hace poco operativo para resolver ahora la cuestión el apoyo en la Jurisprudencia Contencioso-Administrativa*.".

sistemas de información, el Jefe del Negociado de la Unidad de Servicios Sociales de una Junta Municipal, que accedía a datos del Padrón municipal[803], el Jefe de Negociado de Inscripción de Empresa, Afiliación, Altas y Bajas y Variaciones de Datos de los trabajadores[804], o el Sargento de la Guardia Civil que accedió a la base de datos oficial de la Guardia Civil a fin de obtener, para fines privados, datos reservados de terceras personas, cuyos datos, además, fueron utilizados por el acusado a fin de amedrentar a los perjudicados[805].

Todos ellos, con independencia de su calificación administrativa, de tal manera que en la definición penal también se incluye a los funcionarios de hecho que realizan funciones públicas, así como a los interinos y sustitutos. Esto supone realizar una interpretación del término acorde con cada caso concreto, atendiendo a que el sujeto participe de forma temporal o permanente en funciones públicas, habiendo sido designado para su ejercicio[806].

---

803 STS, Sala Segunda, de 11 de julio de 2001, nº 1461/2001, recurso 3323/1999, Pte. Excmo. Sr. D. José Ramón Soriano Soriano (EDJ 2001/16167).

804 STS de 17 de junio de 2014, *cit*., nota 535.

805 SAP de Valencia, Sección 3ª, de 4 de mayo de 2012, nº 335/2012, recurso 89/2011, Pte. Ilma. Sra. Dª Lucía Sanz Díaz (JUR 2012\286929).

806 Como dice la STS, Sala Segunda, de 23 de mayo de 2005, nº 663/2005, Pte. Excmo. Sr. D. Juan Ramón Berdugo y Gómez de la Torre (RJ 2005\7339), con cita de otras, en su FD 16º: "*Así pues, «la cualidad de funcionario a efectos penales no puede subordinarse, ni hacerse depender de su vinculación o calificación administrativa, ni de las definiciones contenidas en las normas reguladoras de su relación con la Administración Pública, sino que ha de atenderse al art. 119 del Código Penal (RCL 1995,*

Ciertamente, el citado concepto es más estricto del que podemos encontrar, por ejemplo en el artículo 615 *ter* del Código penal italiano[807], donde junto al tipo básico de *hacking* se regula como agravante el intrusismo informático llevado a cabo por un funcionario público o encargado de servicio público, con abuso de poder o con violación de los deberes inherentes a su cargo, o abusivamente por detective privado o con abuso de la cualidad de operador del sistema, abarcando de esta forma un abanico más amplio que las conductas del artículo 198 del CP español, que sólo regula las conductas llevadas a cabo por autoridad o funcionario público.

Son por tanto los citados sujetos los afectados por la agravante, que no comprendería otros casos como los encargados de servicios públicos, detectives privados u operadores del sistema, y que en el artículo 198 CP parece coherente no incluir para de esta forma seguir la citada definición del artículo 24 CP y evitar una excesiva ampliación del tipo, contraria al principio de legalidad.

---

*3170 y RCL 1996, 777), que sólo hace depender tal cualidad del hecho concreto y real que una persona se halle participando más o menos permanente o temporalmente habiendo sido designada para ello en el ejercicio de funciones públicas». (STS 8.5.92 [RJ 1992, 3770]). Y así han de incluirse «los llamados funcionarios de hecho que desempeñan una función pública, aunque no reúnan todas las calificaciones o legitimaciones requeridas» ( STS 30.9.92 [ RJ 1992, 7409]), así como internos, sustitutos, pues «los funcionarios de empleo», en contraposición de los funcionarios de carrera, tienen similar cuadro de derechos y obligaciones que los recogidos en el propio Estatuto de los funcionarios de propiedad (SSTS 20.5.93 [RJ 1993, 4189] y 9.10.91 [RJ 1991, 7587])*".

807 *Vid., supra* Capítulo II, subepígrafe 4.11.

### *3.2 La actuación "fuera de los casos permitidos por la Ley".*

En segundo lugar, la exigencia de que la conducta sea llevada a cabo fuera de los casos permitidos por la Ley, implica que la autoridad o funcionario público comete el intrusismo informático en el ejercicio de sus funciones pero la realización de la conducta no debe tener cobertura legal, es decir, como indica GONZÁLEZ CUSSAC, al igual que otros delitos especiales impropios como las detenciones ilegales del artículo 167 CP, el sujeto obra fuera de sus competencias, como un particular, pero con prevalimiento de la condición especial que ostenta[808], siendo evidente que actúa fuera de la ley y, en consecuencia, fuera de sus competencias[809].

La autoridad o funcionario público no debe estar autorizada para acceder a todo o parte del sistema de información, facilitar el acceso o mantenerse en el sistema. Así lo recordaba, con ocasión de un caso de revelación de secretos, la STS de 3 de mayo de 2013[810], relativa a un supuesto de un Inspector de Policía que remitía a otros compañeros un correo electrónico con detalles del fallecimiento de un

---

808 GONZÁLEZ CUSSAC, J. L., "Delitos contra la intimidad ...", *cit*., nota 763, pp. 288 y 289.

809 CARBONELL MATEU, J. C., y GONZÁLEZ CUSSAC, J. L., "Artículo 167", en VIVES ANTÓN, T. (Coord.) y VVAA, *Comentarios al Código Penal de 1995*, ed. Tirant Lo Blanch, Valencia, 1996 (libro electrónico sin numeración de páginas).

810 STS, Sala Segunda, de 3 de mayo de 2013, nº 377/2013, recurso 1041/2012, Pte. Excmo. Sr. D. Miguel Colmenero Menéndez de Luarca (EDJ 2013/55362).

Subinspector, si bien sin percatarse de ello y siendo absuelto por su comisión culposa, declarando en su FD 2º la ilegalidad en el acceso en el caso del artículo 198 CP en los siguientes términos:

"*La diferencia esencial entre las conductas contempladas en los artículos 197 y 198 y el 417, cometidas por un funcionario o autoridad, se centra en la legalidad del acceso a la información reservada a la que se refieren dichos preceptos. El artículo 197 parte de la exigencia de que el autor no esté autorizado para el acceso, el apoderamiento, la utilización o la modificación en relación a los datos reservados de carácter personal o familiar, castigándose en el artículo 198 a la autoridad o funcionario público que, fuera de los casos permitidos por la ley, sin mediar causa legal por delito y prevaliéndose de su cargo, realizare cualquiera de las conductas descritas en el artículo anterior. Mientras que el artículo 417 castiga la revelación de secretos o informaciones que no deban ser divulgados, y de los que la autoridad o funcionario público haya tenido conocimiento por razón de su oficio o cargo*".

La citada autorización para el acceso puede proceder del titular de los datos o de las personas competentes para recabarlos y obtenerlos, tal y como se establecía en la STS de 11 de julio de 2001[811], que condenaba por un delito de descubrimiento de secretos por funcionario público del anterior artículo 197.2 CP al acusado que "*se apoderó, obteniéndolos a través de su ordenador, de datos personales reservados del Padrón Municipal*", accediendo a los datos

[811] STS de 11 de julio de 2001, FJ 3º, *cit*., nota 803.

por medio de las claves de acceso de dos compañeros, por tanto "*haciéndolo por cauces no autorizados*" porque "*no ha acreditado que tuviese autorización del titular de los datos, o fuera de las personas, que tratándose de los casos previstos en la normativa vigente en el momento de la comisión de los hechos (Ley Orgánica núm. 5 de Regulación del Tratamiento Automatizado de Datos de carácter personal de 29 de octubre de 1992: LORTAD) tuvieran competencia para recabarlos y obtenerlos, ni lo hizo en la forma reglamentariamente establecida (art. 7 de la LORTAD)*".

También es posible que la autorización se derive del ámbito de un expediente comprendido en el ámbito concreto de sus funciones que pueda justificar el acceso, conforme la STS de 17 de junio de 2014[812], donde se establecía que "*La autorización que tenía por razón del servicio sólo abarcaba la actuación que le correspondía en el desempeño de las funciones que tenía encomendadas, y no los accesos que hiciera al margen de éstas*", precisando que "*Una cosa es que en su condición de funcionario de la Tesorería de la Seguridad Social estuviera autorizado para acceder a determinadas bases, y otra es que esa autorización ampare el acceso a tales bases al margen de cualquier expediente o actuación oficial*", y condenaba conforme al artículo 198 CP, si bien en relación con el artículo 197.2 CP atendida la fecha de los hechos, al funcionario que estaba habilitado "*para acceder a las bases relativas a contenidos específicos, en concreto las que se veían afectadas por las tareas que tenía asignadas "el registro*

812 La STS de 17 de junio de 2014, *cit*., nota 535, FJ 4º.

*de entrada y salida de escritos y oficios, el desplazamiento al extranjero de trabajadores y la emisión de certificados de deuda de profesionales taurinos". Estaba autorizado para acceder a éstas, pero solo en el ejercicio de las funciones de su cargo, es decir, estaba justificado el acceso que exigía su actuación como funcionario, pero no otros, ni en estas bases, y aun menos en otras como aquellas de las que extrajo los datos que transmitió a terceros*", concluyendo que "*el acusado no estaba autorizado para consultar las 8936 veces que lo hizo, los datos de trabajadores, empresas, vida laboral, prestaciones y certificados de situación de cotización, que posteriormente trasmitió".* El funcionario, tal y como concluye el FJ 8º de la STS, *"operó al margen de cualquier expediente que pudiera justificar las transacciones o consultas que realizó*".

De esta forma, para la conducta del artículo 198 es necesario el elemento de la falta de autorización, que es independiente de la condición de autoridad o funcionario público que se ha analizado más arriba[813]. Por tanto, a los efectos de estos supuestos, es irrelevante la condición de autoridad o agente de la autoridad para entender que concurre un acceso ilícito al sistema de información, incluso si se trata de un sargento de la Guardia Civil que accede a la base de datos del Cuerpo, o que se utilice la clave de acceso asignada por razón del cargo para llevar a cabo el acceso al sistema de información, por cuanto el acceso debe realizarse para el ejercicio de las funciones propias de ese cargo.

[813] *Vid., supra* epígrafe 3.1 de este Capítulo.

Son ejemplos de estos últimos casos citados:

- la SAP de Valencia de 4 de mayo de 2012, que condena al Sargento de la Guardia Civil por un delito de descubrimiento y revelación de secretos por el acceso a la base de datos de la Guardia Civil sin autorización, accediendo a datos reservados de terceras personas con los que pretendía amedrentar a los perjudicados, a pesar de que "*La defensa pretende que la condición de agente de la guardia civil del acusado era bastante para llevar a cabo el acceso que se le reprocha. Para ello invoca que el acceso se produjo dentro del ejercicio de aquella función y alega la Ley 2/1986, de las Fuerzas y Cuerpos de Seguridad del Estado, la que habilita a los agentes de los distintos cuerpos para el seguimiento y persecución de los delitos y le impone la obligación de ejercitar tales funciones, reconduciendo su alegato a los dispueto en su artículo 11, apartados g ) ("investigar delitos para descubrir y detener a lso presuntos culpables....." ) y h) ("captar, recibir y analizar cuantos datos tengan interés para el orden y la seguridad pública y estudiar, planificar y ejecutar los métodos y técnicas de prevención de la delincuencia*", porque *"ni el acusado había procedió a denunciar los hechos que motivaron que se sintiera engañado, ni comunicó a sus superiores el hecho, sin*

*que el testimonio prestado por el agente con TIP NUM015 en el juicio oral, pueda llevarnos a conclusión diferente y ello por cuanto el expresado agente -Jefe directo del acusado- manifestó que éste "no le contó haber sido víctima de una estafa..." , añadiendo seguidamente que " en el mes de junio le dijo que le habían engañado... ", sin mayor concreción, no pudiendo olvidar que en el mes de junio (16-6-2009) fue detenido el acusado y, por tanto, a lo largo de dicho mes, aquel se hubiera enterado, de una u otra forma, de cual era al versión de los hechos del acusado con respecto a los hechos acaecidos el día 17- 4-2009; y, en cualquier caso, al margen del acceso no autorizado a las repetidas bases el día 5-6-2009, no puede pasarse por alto que fue en el mes anterior (mayo) cuando se llevaron a efecto las reiteradas consultas más arriba mencionadas"*[814].

- La STS de 17 de junio de 2014, que contradice el criterio de la Audiencia Provincial de Valladolid, que había considerado que "*el mismo tenía autorizado el acceso, ya que las consultas a las bases de datos de las que obtuvo la información que luego transmitió a terceros, las realizó mediante el empleo de su clave personal que permitía entrar a las mismas, sin*

[814] SAP de Valencia de 4 de mayo de 2012, *cit*., nota 805, FJ 3º.

*perjuicio de que por la asignación de funciones en la oficina le correspondieran tareas de otras áreas*", y en su FD 4º declara que "*La autorización que tenía por razón del servicio sólo abarcaba la actuación que le correspondía en el desempeño de las funciones que tenía encomendadas, y no los accesos que hiciera al margen de éstas. Una cosa es que en su condición de funcionario de la Tesorería de la Seguridad Social estuviera autorizado para acceder a determinadas bases, y otra es que esa autorización ampare el acceso a tales bases al margen de cualquier expediente o actuación oficial*"[815].

En definitiva, la falta de cobertura legal en el acceso al sistema de información determina también la conducta del artículo 198.

---

[815] STS de 17 de junio de 2014, *cit*., nota 535.

En el mismo sentido, la STS de 3 de febrero de 2009, *cit*., nota 792, en su FD 4º, respecto a un agente de Policía, declaraba que "*El recurrente pretende que la condición de agente de policía que tenía el acusado era bastante para llevar a cabo el acceso que se le reprocha. Para ello invoca que el acceso se produjo dentro del ejercicio de aquella función.*

*No obstante, como razona la recurrida, no cabe amparar el acceso en la supuesta búsqueda de datos para constatar la comisión por los titulares de los datos reservados de un delito de estafa. Porque no existen datos sobre el inespecífico hecho supuestamente constitutivo de tal delito, ni precedió denuncia alguna, ni el acusado comunicó a la institución la existencia de tal sospecha de delito para que se incoasen las diligencias oportunas*".

### *3.3 La actuación "sin mediar causa legal por delito".*

La causa por delito existe, tal y como indica CLIMENT DURÁN, "*cuando, constando un hecho delictivo que esté al menos racionalmente indiciado y que sea imputable a una o varias personas, se produce una actuación policial o judicial dirigida a la averiguación de ese hecho o al aseguramiento de la persona o personas presuntamente responsables*"[816].

Así, siguiendo a CARBONELL MATEU y GONZÁLEZ CUSSAC, se trataría de una "*actuación ilegal, ilegítima, fuera totalmente del Derecho, y por tanto del ejercicio correcto de la funcion pública*"[817].

Aunque algunos autores como FRÍAS MARTÍNEZ[818] han criticado este elemento por considerarlo redundante e inexacto en la medida en que los distintos tipos ya fijan esa excepción al regular los requisitos de cada delito, podemos entender que la exigencia de que

---

816 CLIMENT DURÁN, C., "Título XXI. Delitos contra la Constitución. Capítulo V. De los delitos cometidos por los funcionarios públicos contra las garantías constitucionales. Sección 1ª. De los delitos cometidos por los funcionarios públicos contra la libertad individual", en GÓMEZ TOMILLO, M. (Dir.) y VVAA, *Comentarios al Código Penal ...*, *cit*., nota 124, p. 1822.

817 CARBONELL MATEU, J. C., y GONZÁLEZ CUSSAC, J. L., "Artículo 167", *cit*., nota 809, (libro electrónico sin numeración de páginas). En el mismo sentido, GONZÁLEZ CUSSAC, J. L., "Delitos contra la libertad", en GONZÁLEZ CUSSAC, J.L. (Coord.), y VVAA, *Derecho penal. Parte especial*, ed. Tirant Lo Blanch, Valencia, 2016, p. 146.

818 FRÍAS MARTÍNEZ, E., "Delitos contra la intimidad ...", *cit*., nota 529, p. 371.

no medie causa legal por delito, siguiendo a JORGE BARREIRO[819] implica que el acceso ilícito al sistema de información no guarde relación con las actividades en un procedimiento en torno a la investigación de un delito, comprendiendo el término causa tanto el procedimiento iniciado por una autoridad judicial como las diligencias que pudiera llevar a cabo la policía judicial para la comprobación de hechos que pudieran constituir delito o la averiguación de su autor.

La existencia del procedimiento judicial o las diligencia policiales serán las que determinen si media causa por delito y por tanto la conducta es encuadrable en el artículo 198. De esta forma, mientras en el supuesto del citado artículo 536 CP se actúa mediando causa por delito, como indica TOMÁS-VALIENTE LANUZA[820], en el caso que nos ocupa el funcionario actúa completamente al margen de la legalidad, sin existir tampoco investigación por delito, argumento que trasladado al *hacking* implicaría que la autoridad o funcionario público accedería al sistema informático, facilitaría el acceso o permanecería en el sistema sin investigación instada por la autoridad judicial o por el Ministerio fiscal o en el ámbito de unas diligencias policiales iniciadas por la posible comisión de un delito.

No obstante, según expone MORALES PRATS, también sería posible que mediase causa penal sobre un sujeto y, fuera de esa investigación, se llevasen a cabo las injerencias en su esfera de

819 JORGE BARREIRO, A., "Delitos contra la intimidad ...", *cit*., nota 117, p. 1039.

820 TOMÁS-VALIENTE LANUZA, C., "Título X. Delitos contra la Intimidad ...", *cit*., nota 127, p. 806.

intimidad por parte de los funcionarios públicos, prevaliéndose de sus funciones[821]. En nuestro caso el acceso a su sistema informático, la permanencia en el sistema o facilitar el acceso con la correspondiente puesta en peligro concreto de su seguridad, supuestos en los que se aplicaría el artículo 198 CP.

### *3.4 La actuación "prevaliéndose de su cargo".*

Por último, los hechos han de producirse con prevalimiento del cargo. Ello significa que el sujeto debe valerse o servirse de algo para ventaja o provecho propio[822], o el aprovechamiento de la función que se realiza para cometer un hecho delictivo con mayor facilidad[823].

De forma más precisa, prevalerse del carácter público del culpable constituye una agravante genérica prevista en el artículo 22.7ª CP, que significa "*abusar el sujeto activo de su condición de*

---

821 MORALES PRATS, F., "Delitos contra la intimidad ...", *cit.*, nota 489, p. 482.

822 Definición ofrecida por la RAE, disponible en http://lema.rae.es/drae/?val=prevalerse, consultado el 8 de octubre de 2015.

823 Esta definición es la contenida en la SAP de Sevilla, Sección 7ª, de 7 de diciembre de 2011, nº 76/2011, recurso nº 6122/2011, Pte. Ilmo. Sr. D. Francisco Javier González Fernández (ARP 2012\151), FD 1º: "*prevalerse supone el aprovechamiento de la función que se realiza para cometer un hecho delictivo con mayor facilidad, sin que se trate de una agravación especial anudada a la función pública, puesto que cualquier servidor público puede cometer cualquier clase de delitos en los que resulta irrelevante su conducción de ejercicio de función pública*".

*autoridad o funcionario público para realizar con mayor facilidad el hecho delictivo*", de tal manera que ese prevalimiento es la "*acción de prevalerse del carácter público, del cargo como autoridad o funcionario público como medio para cometer el delito, circunstancia que opera como agravante genérica en cualquier delito, que aumenta el desvalor objetivo de la acción por la peligrosidad y la vulneración de deberes funcionariales esenciales y también el desvalor del resultado por el daño que hace a la imagen de una recta administración pública, y además opera como requisito o cualificación de en muchos tipos delictivos*" y, en el caso concreto del artículo 198 CP, prevalerse del cargo se define como "*abusar alguien de su condición de autoridad o funcionario público*"[824].

No obstante la referencia del artículo 22.7ª CP, las circunstancias inherentes, siguiendo a QUINTERO OLIVARES, son aquellas sin cuya concurrencia no hubiera podido cometerse el delito[825], razón por la cual, tal y como señala LUZÓN CUESTA[826], la circunstancia agravante del artículo 22.7ª, al ser inherente al mismo, no se puede aplicar al delito que nos ocupa, de conformidad con el artículo 67 CP[827].

---

824 Las citadas definiciones de las agravantes de los artículos 22.7ª y 198 CP están recogidas en MUÑOZ MACHADO, S. (Dir.) y VVAA, *Diccionario del español jurídico …*, *cit*., nota 104, p. 1260.

825 QUINTERO OLIVARES, G., con la colaboración de MORALES PRATS, F., *Parte general …*, cit., nota 464, p. 785.

826 LUZÓN CUESTA, J. M., *Compendio de Derecho Penal …*, *cit*., nota 12, p. 171.

827 Según dispone el artículo 67 CP, "*Las reglas del artículo anterior no*

Como indica POZUELO PÉREZ[828], el prevalimiento como circunstancia agravante tiene su fundamento en el abuso de superioridad del que hace uso el sujeto que comete el delito, de tal forma que utiliza su condición de funcionario o cargo público al servicio del objetivo delictivo y para su propio beneficio, aprovechando las ventajas de su posición para cometer el delito de forma más sencilla y con menor peligro. Así, conforme mantiene FRÍAS MARTÍNEZ, el sujeto actúa con abuso de sus funciones públicas, sea o no en ejercicio de las mismas[829].

En este sentido, señala GONZÁLEZ CUSSAC que el servidor público actúa por completo fuera de sus competencias, es decir, como particular, pero prevaliéndose de su especial condición[830].

Así, en cuanto a la citada agravante genérica la STS de 6 de julio de 1990 en su FJ 7º declaraba que "*La circunstancia referida se refiere expresamente al prevalimiento del carácter público y no al abuso de la función, es decir, que el agente obra como particular más prevaliéndose de las funciones o carácter público que ejerce*,

---

*se aplicarán a las circunstancias agravantes o atenuantes que la Ley haya tenido en cuenta al describir o sancionar una infracción, ni a las que sean de tal manera inherentes al delito que sin la concurrencia de ellas no podría cometerse*".

828 POZUELO PÉREZ, L., "Circunstancias agravantes y mixta de parentesco", en MOLINA FERNÁNDEZ, F. (Coord.) y VVAA, *Memento práctico penal 2017*, ed. Francis Lefebvre, Madrid, 2016, p. 488.

829 FRÍAS MARTÍNEZ, E., "Delitos contra la intimidad ...", *cit*., nota 529, p. 371.

830 GONZÁLEZ CUSSAC, J.L., "Delitos contra la intimidad ...", *cit*., nota 763, pp. 288 y 289.

*haciendo valer su posición oficial para llegar al objeto propuesto, a la realización del proyectado hecho. Aprovecha la cualidad de funcionario, pero no dentro de la actividad que le es inherente, a fin de gozar de una mayor facilidad para conseguir su delictuoso móvil".* De esta forma, según el criterio jurisprudencial, la circunstancia de agravación *"requiere que la condición de funcionario público, en sentido amplio, sea real y además se ponga al servicio del propósito criminal, aprovechándose así de las ventajas que el cargo le ofrezca para ejecutar el hecho delictivo con mayor facilidad y menor riesgo*"[831].

Por tanto, el supuesto del artículo 198 CP supone un abuso de las facultades inherentes a su cargo para llevar a cabo el acceso ilícito[832], facilitarlo o mantenerse en el sistema informático. Cuando se realizan estas conductas, la autoridad o funcionario público infringe un deber funcionarial de conservar la integridad y seguridad de los sistemas de información y, además, infringe otro deber accediendo a todo o parte del sistema ilegalmente, un acceso que no debería

---

831 STS, Sala Segunda, de 6 de julio de 1990, Pte. Excmo. Sr. D. Francisco Soto Nieto (RJ 1990/6254).

832 De conformidad con la STS de 17 de junio de 2014, *cit*., nota 535, FD 1º y 8º, constituye un ejemplo de prevalerse del cargo a los efectos del artículo 198 el funcionario público que "*utilizó para los accesos la clave que tenía asignada para el desempeño de sus funciones*". En ese caso se llevaron a cabo esas "*consultas a datos de trabajadores y de empresas y (…) a vida laboral, prestaciones y certificados de situación de cotización (…) para facilitar esos datos a agentes de la Guardia Civil y Policía Nacional y al jefe de seguridad de El Corte Inglés, con los que tenía relación personal, así como a mutuas laborales*".

producirse por su cargo y que realiza abusando de su posición de autoridad o funcionarial[833], elemento que justifica una mayor pena en estos casos.

Cabe pensar el supuesto en el que la autoridad o funcionario público accede a un sistema informático de forma ilegal, no estando autorizado, precisamente aprovechando que por su cargo tiene conocimiento de las claves de acceso al sistema, haciendo uso de ellas y de esta forma accediendo a todo o parte del mismo, consumando el delito del artículo 198 CP.

También constituye un claro ejemplo de prevalimiento del cargo para la comisión del delito de *hacking* el hacer uso de la tarjeta de acceso que tiene en su poder la autoridad o funcionario público para así llevar a cabo el intrusismo[834], siendo por tanto necesaria en la

---

833 En esta línea, la STS de 11 de junio de 2004, *cit*., nota 798, condenaba a dos funcionarios públicos del INEM que habían accedido indebidamente con sus claves y con las claves de otros funcionarios a datos del lugar de trabajo y domicilio de terceros por un delito de descubrimiento y revelación de secretos, FD 5º: "*mientras en el caso del art. 197.2 CP se trata de un acceso indebido a la fuente de los datos, pues la ley dice "sin estar autorizado", en el caso del art. 417.2 CP el autor tiene un conocimiento propio de su cargo y obtenido por una necesidad del procedimiento administrativo. En ambos casos se vulnera un deber funcionarial de secreto, pero en el supuesto del art. 197.2/198 CP, el funcionario, además, infringe otro deber, dado que él se "apodera" ilegalmente, abusando de su posición funcionarial, de datos que no debería conocer por su cargo. Esta doble infracción de deberes explica y justifica la diferencia de las penas previstas para ambos delitos*.".

834 En este sentido, la STS de 17 de junio de 2014, *cit*., nota 535, declara en su FJ 8º: "*Ya hemos analizado la falta de autorización en la actuación del acusado que operó al margen de cualquier expediente que*

agravante, como indica POZUELO PÉREZ[835], la concurrencia de un elemento objetivo, consistente en la condición de autoridad o funcionario público que tiene el sujeto activo y un elemento subjetivo, que comprendería el uso de ese carácter público, prevaliéndose de su condición, es decir, un "*ánimo de aprovecharse de la condición pública*", exigiéndose que ese uso sobrepase la actuación pública y vaya dirigido a la consecución de fines privados. Por ello, siguiendo a MORALES PRATS, si la autoridad o funcionario público no se prevaliera de su cargo, aun constando una investigación criminal por delito sobre el sujeto, habría que acudir al delito de particulares[836].

### *3.5 Punto de vista personal.*

Se han analizado en este punto los aspectos relativos a la conducta prevista en el artículo 198, considerando como punto de partida la dificultad para su aplicación práctica para el caso del intrusismo informático, por cuanto, aunque algunos autores han extendido el campo del artículo 198 CP a todas las modalidades del

---

*pudiera justificar las transacciones o consultas que realizó. Para ello se prevalió de su cargo, tanto que utilizó para los accesos la clave que tenía asignada para el desempeño de sus funciones*".

835 POZUELO PÉREZ, L., "Circunstancias agravantes ...", *cit*., nota 828, p. 488.

836 MORALES PRATS, F., "Delitos contra la intimidad ...", *cit.*, nota 489, p. 482.

artículo 197 CP[837], la taxatividad del tipo impuesta por el principio de legalidad conlleva su inaplicación práctica al supuesto del artículo 197 *bis* 1 CP, ya que tras la reforma de la LO 1/2015, el anterior artículo 197 pasa a dividirse en varios artículos, mientras el artículo 198 CP sigue manteniendo la misma redacción, es decir, sólo se aplica a la autoridad o funcionario público que "*realizare cualquiera de las conductas descritas en el artículo anterior*". Esto significa su única aplicación a los supuestos del artículo 197 *quinquies*, relativo a la responsabilidad de la persona jurídica. La situación entiendo que se presenta como un error del legislador al no reformar el artículo 198 a la vez que modificaba el artículo 197 con la LO 1/2015 y supone establecer una barrera para los órganos jurisdiccionales que tienen que aplicarlo, en la medida que cuando se les presente el caso de una autoridad o funcionario público que cometa el delito que estamos estudiando, no podrán realizar una interpretación extensiva y analógica del precepto porque "*Las leyes penales no se aplicarán a casos distintos de los comprendidos expresamente en ellas*" conforme ordena el artículo 4.1 CP, sino que, según ese mismo precepto deberán, en su caso, exponer al Gobierno las razones que le asistan para creer que debiera ser objeto de sanción penal.

No obstante, la agravante se ha analizado en este trabajo desde el punto de vista de su aplicación futura a los supuestos de intrusismo informático.

---

837 En este sentido, ANARTE BORRALLO, E. y DOVAL PAIS, A., "Delitos contra la intimidad ...", *cit*., nota 380, p. 535.

Considero que el precepto en cuestión guarda similitud con los artículos 414, 415 o 536 CP.

En el caso del artículo 414 CP se exige que se trate del acceso a documentos y no meramente a un sistema informático que pudiera contenerlos, por ello entiendo que su especialidad y mayor gravedad determina que se deberá resolver a su favor un hipotético concurso de normas con las conductas de facilitar el acceso a un sistema del artículo 197 *bis* 1 CP.

Por su parte, en el artículo 415 CP se puede plantear el caso de que los documentos secretos se encuentren en un sistema informático. En este supuesto, siguiendo el criterio de ANARTE BORRALLO y DOVAL PAÍS con ocasión del anterior artículo 197.3 en relación con el artículo 197.2 CP, considero que se aplicaría el criterio de la consunción del delito cuyo umbral típico se ubica más lejos de la afección al bien jurídico protegido[838] y por tanto, en este caso, estando más lejos el artículo 198 CP, el concurso de normas se resolvería a favor del artículo 415 CP, criterio también mantenido por ROMEO CASABONA, que se refiere a la mayor especialidad en las conductas del artículo 415, a la vista de que el deber infringido por el funcionario es más específico[839], resolviendo el concurso de leyes a favor de este último precepto.

---

838 ANARTE BORRALLO, E. y DOVAL PAIS, A., "Límites de la ley penal ...", *cit*., nota 24, p. 31.

839 ROMEO CASABONA, C. M., *Los delitos de descubrimiento …*, *cit*., nota 791, página 6.

Por lo que respecta al artículo 536 CP, el artículo 198 CP tiene la peculiaridad de que, en relación con las conductas de *hacking* que nos ocupan, además de requerir el acceso al sistema informático, exigiría que la autoridad o funcionario público actuase "*fuera de los casos permitidos por la Ley*", "*sin mediar causa legal por delito*" y "*prevaliéndose de su cargo*". A todo ello se añadiría la circunstancia indicada por GONZÁLEZ CUSSAC de falta de conducta pluriofensiva en el artículo 198 CP[840]. Este autor apunta, junto a CARBONELL MATEU, la posibilidad de un concurso de leyes entre ambos supuestos[841]. Sin embargo, entiendo con ROMEO CASABONA que los supuestos típicos del artículo 536 y del artículo 198 están claramente delimitados, por lo que en puridad no parece que pueda plantearse un concurso de normas[842]. De esta forma, podrían ocurrir situaciones tales como que la autoridad o funcionario público intercepte las telecomunicaciones o utilice alguno de los artificios citados en el artículo 536 CP para de esta forma acceder al sistema informático, supuestos en los que habría que analizar la concurrencia de las citadas circunstancias que integran el tipo del artículo 536 o del 198 CP para resolver la aplicación de uno u otro precepto.

---

840 GONZÁLEZ CUSSAC, J. L., "Delitos contra la intimidad ...", *cit*., nota 763, p. 289.

841 CARBONELL MATEU, J. C., y GONZÁLEZ CUSSAC, J. L., "Artículo 198", *cit*., nota 795 (libro electrónico sin numeración de páginas).

842 ROMEO CASABONA, C. M., *Los delitos de descubrimiento ..., cit*., nota 791, página 6.

En el caso del artículo 198 CP entiendo evidente que el precepto contiene un delito especial impropio o alternativa típica agravada por las características del autor, por cuanto el delito de *hacking* puede ser cometido por cualquiera, siendo por tanto común, pero se agravaría en el artículo 198 CP para el caso de que sea cometido por autoridad o funcionario público.

De esta forma, resulta que, como dice MOLINA FERNÁNDEZ[843], si intervienen varios sujetos, cada uno deberá responder conforme a su hecho y culpabilidad, es decir, conforme al artículo 65 CP, esto significa que la autoridad o funcionario público responderá conforme al artículo 198 CP y quien no tenga esa condición quedará sujeto al artículo 197 *bis* 1 CP.

Por tanto, considero acertada la incorporación del artículo 198 en el CP y la necesidad de relacionarlo con los supuestos de acceso ilícito a todo o parte de un sistema de información, facilitar el acceso o el mantenimiento no autorizado en el sistema, poniendo así fin al tratamiento privilegiado para las autoridades o funcionarios públicos que llevaban a cabo injerencias ilegítimas en los derechos y libertades de los ciudadanos, recibiendo ahora un tratamiento agravado respecto al correlativo delito de *hacking* y abandonando de esta forma un incomprensible tratamiento atenuado para estos sujetos tal y como se recordaba en la Exposición de Motivos del CP[844].

---

843 MOLINA FERNÁNDEZ, F., "Autoría y participación ...", *cit*., nota 793, p. 347.

844 *Vid*., *supra* nota 795.

En el artículo 198 CP se toma como punto de partida el concepto normativo de autoridad o funcionario público contenido en el artículo 24 CP, si bien se ha venido matizado jurisprudencialmente al incluir una interpretación del término acorde con cada caso concreto, atendiendo a que el sujeto participe de forma temporal o permanente en funciones públicas, habiendo sido designado para su ejercicio. En cualquier caso, tanto el concepto normativo como su interpretacion resultan más restrictivos que el contenido en el artículo 615 *ter* del Código Penal italiano, tal y como hemos visto en el Capítulo II, donde junto al tipo básico de *hacking* se regula como agravante el intrusismo informático llevado a cabo por un funcionario público o encargado de servicio público, con abuso de poder o con violación de los deberes inherentes a su cargo, o abusivamente por detective privado o con abuso de la cualidad de operador del sistema, abarcando de esta forma un abanico más amplio que las conductas del artículo 198 del CP español, que sólo regula las conductas llevadas a cabo por autoridad o funcionario público, lo que me parece coherente a fin de seguir la citada definición del artículo 24 CP y evitar una excesiva ampliación del tipo, contraria al principio de legalidad.

Por lo que respecta a la actuación *"fuera de los casos permitidos por la Ley"*, entiendo, siguiendo a GONZÁLEZ CUSSAC, que al igual que otros delitos especiales impropios como las detenciones ilegales del artículo 167 CP, el sujeto obra fuera de sus competencias, como un particular, pero con prevalimiento de la

condición especial que ostenta[845], es decir, que siguiendo también el criterio jurisprudencial, la autoridad o funcionario público no debe estar autorizada para acceder a todo o parte del sistema de información, bien por el titular de los datos o de las personas competentes para recabarlos y obtenerlos.

En definitiva, la falta de cobertura legal en el acceso al sistema de información determina también la conducta del artículo 198.

Además, el citado precepto exige que no medie causa legal por delito en el acceso al sistema informático por parte de la autoridad o funcionario público.

Aunque algunos autores como FRÍAS MARTÍNEZ[846] han criticado este elemento por considerarlo redundante e inexacto en la medida en que los distintos tipos ya fijan esa excepción al regular los requisitos de cada delito, entiendo que es necesario incluirlo para distinguirlo de otros supuestos, como el del citado artículo 536 CP. Asi, sigo a JORGE BARREIRO[847] para entencer que el acceso ilícito al sistema de información no debe guardar relación con las actividades en un procedimiento en torno a la investigación de un delito, comprendiendo el término causa tanto el procedimiento iniciado por una autoridad judicial como las diligencias que pudiera llevar a cabo

845 GONZÁLEZ CUSSAC, J.L., "Delitos contra la intimidad ...", *cit*., nota 763, pp. 288 y 289.

846 FRÍAS MARTÍNEZ, E., "Delitos contra la intimidad ...", *cit*., nota 529, p. 371.

847 JORGE BARREIRO, A., "Delitos contra la intimidad ...", *cit*., nota 117, p. 1039.

la policía judicial para la comprobación de hechos que pudieran constituir delito o la averiguación de su autor.

Por tanto, nos encontraríamos ante otro elemento distintivo con las conductas del arículo 536, tal y como se ha expuesto al principio de este punto, en la medida que en este último caso se actúa mediando causa por delito. Considero que la existencia del procedimiento judicial o las diligencias policiales serán las que determinen si concurre esta circunstancia y por tanto la conducta es encuadrable en el artículo 198, como sucedería si la autoridad o funcionario público accediera al sistema informático, facilitase el acceso o permaneciera en el sistema sin autorización, sin investigación instada por la autoridad judicial o por el Ministerio fiscal o en el ámbito de unas diligencias policiales iniciadas por la posible comisión de un delito. Todo ello no excluye que, como indica MORALES PRATS, mediase causa penal sobre un sujeto y, fuera de esa investigación, se llevasen a cabo las injerencias[848], que entiendo, en relación con el *hacking* y siguiendo el bien jurídico expuesto en el Capítulo III, deberían acaecer en la seguridad del sistema, supuestos en los que se aplicaría también el artículo 198 CP.

Por último, los hechos han de producirse con prevalimiento del cargo, circunstancia que considero inherente al delito del artículo 198 CP y por tanto impide la aplicación de la agravante genérica del artículo 22.7ª CP. Para esta consideración, entiendo que las

[848] MORALES PRATS, F., "Delitos contra la intimidad ...", *cit.*, nota 489, p. 482.

circunstancias inherentes, siguiendo a QUINTERO OLIVARES, son aquellas sin cuya concurrencia no hubiera podido cometerse el delito[849]. Además, conforme mantiene FRÍAS MARTÍNEZ, considero que en estos casos el sujeto actúa con abuso de sus funciones públicas, sea o no en ejercicio de las mismas[850], es decir, que como señala GONZÁLEZ CUSSAC el servidor público actúa por completo fuera de sus competencias, como particular, pero prevaliéndose de su especial condición[851].

Desde mi punto de vista, son ejemplos de los citados supuestos los de la autoridad o funcionario público que accede al sistema informático de forma ilegal, no estando autorizado, sin mediar causa por delito, y realiza la conducta precisamente aprovechando que por su cargo tiene conocimiento de las claves de acceso al sistema, haciendo uso de ellas y de esta forma accediendo a todo o parte del mismo, consumando el delito del artículo 198 CP, o el hacer uso de la tarjeta de acceso que tiene en su poder la autoridad o funcionario público para así llevar a cabo el intrusismo[852]. Por tanto, entiendo

---

849 QUINTERO OLIVARES, G., con la colaboración de MORALES PRATS, F., *Parte general* ..., cit., nota 464, p. 785.

850 FRÍAS MARTÍNEZ, E., "Delitos contra la intimidad ...", *cit*., nota 529, p. 371.

851 GONZÁLEZ CUSSAC, J. L., "Delitos contra la intimidad ...", *cit*., nota 763, pp. 288 y 289.

852 En este sentido, la STS de 17 de junio de 2014, *cit*., nota 535, declara en su FJ 8º: "*Ya hemos analizado la falta de autorización en la actuación del acusado que operó al margen de cualquier expediente que pudiera justificar las transacciones o consultas que realizó. Para ello se prevalió de su cargo, tanto que utilizó para los accesos la clave que tenía*

necesario en la agravante, siguiendo a POZUELO PÉREZ[853], la concurrencia de un elemento objetivo, consistente en la condición de autoridad o funcionario público que tiene el sujeto activo y un elemento subjetivo, que comprendería el uso de ese carácter público, prevaliéndose de su condición, es decir, un "*ánimo de aprovecharse de la condición pública*". Por ello, como indica MORALES PRATS[854], si la autoridad o funcionario público no se prevaliera de su cargo, aun constando una investigación criminal por delito sobre el sujeto, habría que acudir al tipo común.

*asignada para el desempeño de sus funciones*".

853 POZUELO PÉREZ, L., "Circunstancias agravantes ...", *cit*., nota 828, p. 488.

854 MORALES PRATS, F., "Delitos contra la intimidad ...", *cit.*, nota 489, p. 482.

# CAPÍTULO VI.

# RESPONSABILIDAD PENAL DE LAS PERSONAS JURÍDICAS EN EL DELITO DE *HACKING*.

## *1. INTRODUCCIÓN.*

Una vez expuestos los elementos de la figura de *hacking* incluidos en el artículo 197 *bis* 1 CP, su fundamento y naturaleza como delito de peligro y de resultado, el objeto material, bien jurídico, *iter criminis*, las cuestiones concursales y los tipos agravados de los artículos 197 *quater* y 198 CP, se realiza una aproximación en el presente Capítulo a la responsabilidad penal de las personas jurídicas por estas conductas.

Se trata de una novedad introducida con la LO 5/2010, que constituye un supuesto distinto a la comisión de estos delitos en el seno de una organización o grupo criminal, previsto en el artículo 198 CP, y al que se ha hecho referencia en el Capítulo anterior, razón por la cual se hace preciso delimitar la citada materia en este apartado.

La responsabilidad penal de las personas jurídicas se introduce como se ha indicado a través de la citada LO 5/2010, siendo nuevamente modificada por la LO 1/2015.

El ámbito al que se refiere esa responsabilidad puede estar sujeto, en palabras de NIETO MARTÍN y GARCÍA MORENO, a un modelo de *numerus clausus* en el que las personas jurídicas únicamente pueden ser consideradas responsables de la comisión de determinados delitos, o bien un sistema de responsabilidad penal de las personas jurídicas por cualquier infracción prevsta en la legislación

penal[855]. Son ejemplos del primer modelo Portugal, tras su reforma del Código penal de 2007[856] o Italia, que establece un sistema de responsabilidad administrativa derivada de los delitos que sean cometidos en su interés o ventaja[857], a diferencia de los supuestos de

[855] NIETO MARTÍN, A. y GARCÍA MORENO, B., "Derecho penal europeo y comparado. Cooperación judicial", en JUANES PECES, A. (Dir.) y VVAA, *Memento Experto. Responsabilidad penal y procesal de las personas jurídicas*, ed. Francis Lefebvre, Madrid, 2015, p. 27.

[856] La Lei nº 59/2007, de 4 de septiembre, de Vigésima terceira alteração ao Código Penal, aprovado pelo Decreto-Lei n.o 400/82, de 23 de Setembro, disponible en https://www.dgs.pt/accao-de-saude-para-criancas-e-jovens-em-risco/legislacao-relacionada/lei-n-592007-de-4-de-setembro.aspx, consultado el 24 de abril de 2017. Esta Ley establece la responsabilidad de las personas jurídicas en los casos expresamente previstos.

Y artículo 9 de la Lei n.º 109/2009, de 15 de septiembre, de transposición de la DM 2005/222/JAI y el Convenio Europeo sobre Cibercriminalidad, establece la responsabilidad penal de las personas jurídicas por el delito de *hacking*. *Vid.*, *supra* nota 219.

[857] La responsabilidad administrativa derivada del delito está regulada en el Decreto Legislativo de 8 de junio de 2001, nº 231, "Disciplina della responsabilita' amministrativa delle persone giuridiche, delle societa' e delle associazioni anche prive di personalita' giuridica, a norma dell'articolo 11 della legge 29 settembre 2000, n. 300", publicado en la *Gazzetta Ufficiale* nº 140 del 19 de junio de 2001, disponible en http://www.parlamento.it/parlam/leggi/deleghe/01231dl.htm, consultado el 23 de abril de 2017. Su artículo 5 establece:

"*1. L'ente e' responsabile per i reati commessi nel suo interesse o a suo vantaggio:*

*a) da persone che rivestono funzioni di rappresentanza, di amministrazione o di direzione dell'ente o di una sua unita' organizzativa dotata di autonomia finanziaria e funzionale nonche' da persone che esercitano, anche di fatto, la gestione e il controllo dello stesso;*

*b) da persone sottoposte alla direzione o alla vigilanza di uno dei soggetti di cui alla lettera a).*

responsabilidad penal por cualquier infracción prevista en la legislación penal, como sucede en los casos de Francia[858], Holanda[859] o Bélgica[860].

---

*2. L'ente non risponde se le persone indicate nel comma 1 hanno agito nell'interesse esclusivo proprio o di terzi."*

858 El Código penal francés (*vid*., *supra* nota 266) regula la responsabilidad de las personas jurídicas en el artículo 121.2:

"*Les personnes morales, à l'exclusion de l'Etat, sont responsables pénalement, selon les distinctions des articles 121-4 à 121-7, des infractions commises, pour leur compte, par leurs organes ou représentants.*

*Toutefois, les collectivités territoriales et leurs groupements ne sont responsables pénalement que des infractions commises dans l'exercice d'activités susceptibles de faire l'objet de conventions de délégation de service public.*

*La responsabilité pénale des personnes morales n'exclut pas celle des personnes physiques auteurs ou complices des mêmes faits, sous réserve des dispositions du quatrième alinéa de l'article 121-3*".

859 La responsabilidad de las personas jurídicas está prevista en el artículo 51 del Código penal holandés (*vid., supra* nota 278) en los siguientes términos:

*"1. Strafbare feiten kunnen worden begaan door natuurlijke personen en rechtspersonen.*

*2. Indien een strafbaar feit wordt begaan door een rechtspersoon, kan de strafvervolging worden ingesteld en kunnen de in de wet voorziene straffen en maatregelen, indien zij daarvoor in aanmerking komen, worden uitgesproken:*

*1°. tegen die rechtspersoon, dan wel*

*2°. tegen hen die tot het feit opdracht hebben gegeven, alsmede tegen hen die feitelijke leiding hebben gegeven aan de verboden gedraging, dan wel*

*3°. tegen de onder 1° en 2° genoemden te zamen.*

*3. Voor de toepassing van de vorige leden wordt met de rechtspersoon gelijkgesteld: de vennootschap zonder rechtspersoonlijkheid, de maatschap, de rederij en het doelvermogen".*

860 El Código penal belga (*vid., supra* nota 226) establece la responsabilidad de las personas jurídicas en su artículo 5: "*Toute personne*

En España se sigue el sistema de *numerus clausus*, es decir, se establece una incriminación específica y sólo se castiga a la persona jurídica en aquellos delitos que venga expresamente previsto. Uno de ellos es el relativo al *hacking*.

La sanción venía establecida en el párrafo segundo del anterior artículo 197.3:

"*Cuando de acuerdo con lo establecido en el artículo 31 bis una persona jurídica sea responsable de los delitos comprendidos en*

---

*morale est pénalement responsable des infractions qui sont intrinsèquement liées à la réalisation de son objet ou à la défense de ses intérêts, ou de celles dont les faits concrets démontrent qu'elles ont été commises pour son compte.*

*Lorsque la responsabilité de la personne morale est engagée exclusivement en raison de l'intervention d'une personne physique identifiée, seule la personne qui a commis la faute la plus grave peut être condamnée. Si la personne physique identifiée a commis la faute sciemment et volontairement, elle peut être condamnée en même temps que la personne morale responsable.*

*Sont assimilées à des personnes morales:*

*1° les associations momentanées et les associations en participation;*

*2° les sociétés visées à l'article 2, alinéa 3, des lois coordonnées sur les sociétés commerciales, ainsi que les sociétés commerciales en formation;*

*3° les sociétés civiles qui n'ont pas pris la forme d'une société commerciale.*

*Ne peuvent pas être considérées comme des personnes morales responsables pénalement pour l'application du présent article : l'Etat fédéral, les régions, les communautés, les provinces, [les zones de secours,] [ les prézones] l'agglomération bruxelloise, les communes, (les zones pluricommunales,) les organes territoriaux intra-communaux, la Commission communautaire française, la Commission communautaire flamande, la Commission communautaire commune et les centres publics d'aide sociale ".*

*este artículo, se le impondrá la pena de multa de seis meses a dos años. 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*"[861].

[861] El artículo 33.7, letras b) a g), tras la reforma de la LO 5/2010 establece: "*7. Las penas aplicables a las personas jurídicas, que tienen todas la consideración de graves, son las siguientes: (…) b) Disolución de la 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. 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. La intervención podrá afectar a la totalidad de la organización o limitarse a alguna de sus instalaciones, secciones o unidades de negocio. El Juez o Tribunal, en la sentencia o, posteriormente, mediante auto, determinará exactamente el contenido de la intervención y determinará quién se hará cargo de la intervención y en qué plazos deberá realizar informes de seguimiento para el órgano judicial. La intervención se podrá modificar o suspender en todo momento previo informe del interventor y del Ministerio Fiscal. El interventor tendrá derecho a acceder a todas las instalaciones y locales de la empresa o persona jurídica y a recibir cuanta información estime necesaria para el ejercicio de sus funciones. Reglamentariamente se determinarán los aspectos relacionados con el ejercicio de la función de interventor, como la retribución o la cualificación necesaria. La clausura temporal de los locales o establecimientos, la suspensión de las actividades sociales y la intervención judicial podrán ser*

De esta forma, el legislador cumplía con la exigencia del artículo 8 de la DM 2005/222/JAI, que ordenaba a los Estados miembros que incluyeran la responsabilidad de las personas jurídicas en estas conductas de intrusismo informático, tipificadas en su artículo 2 en los siguientes términos:

"*1. Cada Estado miembro adoptará las medidas necesarias para que a las personas jurídicas se les puedan exigir responsabilidades por las infracciones mencionadas en los artículos 2, 3, 4 y 5, cuando dichas infracciones sean cometidas en su beneficio por cualquier persona, actuando a título particular o como parte de un órgano de la persona jurídica, que ostente un cargo directivo en el seno de dicha persona jurídica basado en: a) un poder de representación de dicha persona jurídica, o b) una autoridad para tomar decisiones en nombre de dicha persona jurídica, o c) una autoridad para ejercer un control en el seno de dicha persona jurídica. 2. Sin perjuicio de los casos previstos en el apartado 1, los Estados miembros garantizarán que a las personas jurídicas se les puedan exigir responsabilidades cuando la falta de vigilancia o control por parte de alguna de las personas a que se refiere el apartado 1 haya hecho posible que una persona sometida a su autoridad cometa las infracciones mencionadas en los artículos 2, 3, 4 y 5 en beneficio de esa persona jurídica*".

---

*acordadas también por el Juez Instructor como medida cautelar durante la instrucción de la causa".*

Por tanto, aunque la DM 2005/222/JAI no exigía que la sanción a las personas jurídicas por *hacking* fuese penal, en nuestro ordenamiento jurídico interno se ha optado por tipificarla desde la reforma del año 2010, abandonando el principio "*societas delinquere non potest*" para dar paso al "*societas delinquere et puniri potest*".

La LO 1/2015 ha regulado estas conductas en el nuevo artículo 197 *quinquies* CP, que sustituye al citado artículo 197.3 en su párrafo segundo, y atiende a lo establecido en el artículo 10 de la Directiva 2013/40/UE aunque, al igual que la citada DM 2005/222/JAI, esta norma tampoco exigía la respuesta penal[862]. Esto es debido, entre otras razones, a que no todos los sistemas de sanción de las personas jurídicas son penales, señalando NIETO MARTÍN y GARCÍA MORENO que las sanciones administrativas o la fijación de sanciones de diversa naturaleza a la pena ha sido la fórmula para superar los

[862] El artículo 10 de la Directiva 2013/40/UE establece en sus dos primeros apartados que "*1. Los Estados miembros adoptarán las medidas necesarias para garantizar que las personas jurídicas puedan ser consideradas responsables de las infracciones mencionadas en los artículos 3 a 8 cuando estas infracciones sean cometidas en su beneficio por cualquier persona que, actuando a título particular o como parte de un órgano de la persona jurídica, ostente un cargo directivo en el seno de dicha persona jurídica, basado en: a) el poder de representación de dicha persona jurídica, o b) la capacidad para tomar decisiones en nombre de dicha persona jurídica, o c) la capacidad para ejercer un control en el seno de dicha persona jurídica. 2. Los Estados miembros adoptarán las medidas necesarias para garantizar que las personas jurídicas puedan ser consideradas responsables cuando la falta de supervisión o control por parte de alguna de las personas a que se refiere el apartado 1 haya permitido que una persona sometida a su autoridad cometa una de las infracciones mencionadas en los artículos 3 a 8 en beneficio de esa persona jurídica*".

recelos teóricos a la necesidad de sancionar a las personas jurídicas, viniendo propiciada por la normativa internacional y poniendo el acento en la eficacia y proporcionalidad de las sanciones, no en su *nomen iuris*[863]. Así, en el Derecho comparado encontramos distintos modelos de responsabilidad de la persona jurídica, pudiendo citar, siguiendo a JUANES PECES el sistema de responsabilidad penal como el de Francia[864], sólo adminitrativa en Alemania[865] o el sistema híbrido de Italia[866].

---

863 NIETO MARTÍN, A. y GARCÍA MORENO, B., "Derecho penal europeo ...", *cit*., nota 855, p. 23.

864 En este sentido, *vid., supra* nota 858.

865 El Código de infracciones reglamentarias de 19 de febrero de 1987, disponible en https://www.gesetze-im-internet.de/owig_1968/inhalts_bersicht.html, consultado el 24 de abril de 2017, establece en su artículo 30 la responsabilidad administrativa de las personas jurídicas:

"*Gesetz über Ordnungswidrigkeiten (OWiG)*
*§ 30 Geldbuße gegen juristische Personen und Personenvereinigungen:*

*(1) Hat jemand*

*1. als vertretungsberechtigtes Organ einer juristischen Person oder als Mitglied eines solchen Organs,*

*2. als Vorstand eines nicht rechtsfähigen Vereins oder als Mitglied eines solchen Vorstandes,*

*3. als vertretungsberechtigter Gesellschafter einer rechtsfähigen Personengesellschaft,*

*4. als Generalbevollmächtigter oder in leitender Stellung als Prokurist oder Handlungsbevollmächtigter einer juristischen Person oder einer in Nummer 2 oder 3 genannten Personenvereinigung oder*

*5. als sonstige Person, die für die Leitung des Betriebs oder Unternehmens einer juristischen Person oder einer in Nummer 2 oder 3 genannten Personenvereinigung verantwortlich handelt, wozu auch die Überwachung der Geschäftsführung oder die sonstige Ausübung von Kontrollbefugnissen in leitender Stellung gehört, eine Straftat oder*

*Ordnungswidrigkeit begangen, durch die Pflichten, welche die juristische Person oder die Personenvereinigung treffen, verletzt worden sind oder die juristische Person oder die Personenvereinigung bereichert worden ist oder werden sollte, so kann gegen diese eine Geldbuße festgesetzt werden.*
*(2) Die Geldbuße beträgt*

*1. im Falle einer vorsätzlichen Straftat bis zu zehn Millionen Euro,*

*2. im Falle einer fahrlässigen Straftat bis zu fünf Millionen Euro.*

*Im Falle einer Ordnungswidrigkeit bestimmt sich das Höchstmaß der Geldbuße nach dem für die Ordnungswidrigkeit angedrohten Höchstmaß der Geldbuße. Verweist das Gesetz auf diese Vorschrift, so verzehnfacht sich das Höchstmaß der Geldbuße nach Satz 2 für die im Gesetz bezeichneten Tatbestände. Satz 2 gilt auch im Falle einer Tat, die gleichzeitig Straftat und Ordnungswidrigkeit ist, wenn das für die Ordnungswidrigkeit angedrohte Höchstmaß der Geldbuße das Höchstmaß nach Satz 1 übersteigt.*

*(2a) Im Falle einer Gesamtrechtsnachfolge oder einer partiellen Gesamtrechtsnachfolge durch Aufspaltung (§ 123 Absatz 1 des Umwandlungsgesetzes) kann die Geldbuße nach Absatz 1 und 2 gegen den oder die Rechtsnachfolger festgesetzt werden. Die Geldbuße darf in diesen Fällen den Wert des übernommenen Vermögens sowie die Höhe der gegenüber dem Rechtsvorgänger angemessenen Geldbuße nicht übersteigen. Im Bußgeldverfahren tritt der Rechtsnachfolger oder treten die Rechtsnachfolger in die Verfahrensstellung ein, in der sich der Rechtsvorgänger zum Zeitpunkt des Wirksamwerdens der Rechtsnachfolge befunden hat.*

*(3) § 17 Abs. 4 und § 18 gelten entsprechend.*

*(4) Wird wegen der Straftat oder Ordnungswidrigkeit ein Straf- oder Bußgeldverfahren nicht eingeleitet oder wird es eingestellt oder wird von Strafe abgesehen, so kann die Geldbuße selbständig festgesetzt werden. Durch Gesetz kann bestimmt werden, daß die Geldbuße auch in weiteren Fällen selbständig festgesetzt werden kann. Die selbständige Festsetzung einer Geldbuße gegen die juristische Person oder Personenvereinigung ist jedoch ausgeschlossen, wenn die Straftat oder Ordnungswidrigkeit aus rechtlichen Gründen nicht verfolgt werden kann; § 33 Abs. 1 Satz 2 bleibt unberührt.*

*(5) Die Festsetzung einer Geldbuße gegen die juristische Person oder Personenvereinigung schließt es aus, gegen sie wegen derselben Tat den Verfall nach den §§ 73 oder 73a des Strafgesetzbuches oder nach § 29a anzuordnen.*

En el presente Capítulo se trata de realizar una aproximación a la responsabilidad penal de la persona jurídica cuando se comete el delito de intrusismo informático. En concreto, quiénes deben llevar a cabo las conductas de *hacking* para que nos encontremos en los supuestos del artículo 197 *quinquies* CP.

## *2. RESPONSABILIDAD PENAL DE LA PERSONA JURÍDICA EN EL DELITO DE HACKING.*

### *2.1 Planteamiento.*

El artículo 197 *quinquies* CP establece:

"*Cuando de acuerdo con lo establecido en el artículo 31 bis una persona jurídica sea responsable de los delitos comprendidos en los artículos 197, 197 bis y 197 ter, se le impondrá la pena de multa de seis meses a dos años. 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".*

---

*(6) Bei Erlass eines Bußgeldbescheids ist zur Sicherung der Geldbuße § 111d Absatz 1 Satz 2 der Strafprozessordnung mit der Maßgabe anzuwenden, dass an die Stelle des Urteils der Bußgeldbescheid tritt".*

866 JUANES PECES, A., "Introducción a la responsabilidad penal de las personas jurídicas. Consideraciones generales y problemas sustantivos y procesales que dicha responsabilidad suscita", en JUANES PECES, A. (Dir.) y VVAA, *Memento Experto. Responsabilidad penal y procesal de las personas jurídicas*, ed. Francis Lefebvre, Madrid, 2015, p. 8.

De esta forma, el precepto se remite al artículo 31 *bis* para determinar cuándo una persona jurídica puede ser responsable por los delitos de *hacking*, y el apartado 1 de este artículo se ocupa de delimitar la responsabilidad de las personas jurídicas en dos supuestos distintos relativos a su propio beneficio:

"*1. En los supuestos previstos en este Código, las personas jurídicas serán penalmente responsables: a) De los delitos cometidos en nombre o por cuenta de las mismas, y en su beneficio directo o indirecto, por sus representantes legales o por aquellos que actuando individualmente o como integrantes de un órgano de la persona jurídica, están autorizados para tomar decisiones en nombre de la persona jurídica u ostentan facultades de organización y control dentro de la misma. b) De los delitos cometidos, en el ejercicio de actividades sociales y por cuenta y en beneficio directo o indirecto de las mismas, por quienes, estando sometidos a la autoridad de las personas físicas mencionadas en el párrafo anterior, han podido realizar los hechos por haberse incumplido gravemente por aquéllos los deberes de supervisión, vigilancia y control de su actividad atendidas las concretas circunstancias del caso*".

Por tanto, podemos distinguir dos tipos de comportamientos que pueden motivar la responsabilidad penal de la persona moral: (i) conductas en nombre o por cuenta de ella, por parte de sus representantes legales o quienes están autorizados para tomar decisiones o tienen facultades de organización y control; y (ii) en los supuestos en que se ejercitan actividades sociales y por cuenta de la

persona jurídica, por quienes están sometidos a la autoridad de las personas anteriores.

Como indica DOPICO GÓMEZ-ALLER[867], se trata de incentivar que las personas jurídicas asuman una autoorganización para impedir modelos delictivos con el fin de lograr sus objetivos sociales, intentando así que la persona jurídica sea quien adopte las medidas para investigar y evitar las conductas que le puedan favorecer pero que sean delictivas.

En este sentido, siguiendo a JUANES PECES, la estructura compleja de las empresas dificultaba la investigación de los delitos cometidos en su seno o desplazaba la responsabilidad hacia niveles inferiores. Por ello, se intenta evitar su impunidad y, además de la previsión de una pena, se obliga a las sociedades a asumir determinadas medidas, actuando también desde el plano preventivo[868].

En consecuencia, resultaba necesario introducir esta responsabilidad penal en nuestra legislación, en una materia tan novedosa como los delitos de *hacking*, ya que nos encontramos ante un delito complejo de nuevo cuño, donde continuamente se modifican o perfeccionan las técnicas de intrusismo informático, resultando difícil su prevención y persecución por el Estado. Así, en estos casos

---

867 DOPICO GÓMEZ-ALLER, J., "Responsabilidad de personas jurídicas", en ORTIZ DE URBINA GIMENO, Í. (Coord.) y VVAA, *Memento experto. Reforma penal 2010. Ley Orgánica 5/2010*, ed. Francis Lefebvre, Madrid, 2010, p. 12.

868 JUANES PECES, A., "Introducción a la responsabilidad ...", *cit*., nota 866, p. 8

parecen plenamente válidos los argumentos expuestos por NIETO MARTÍN[869] y seguidos por RIVAS VERDES-MONTEGRO[870] para justificar la responsabilidad penal de la persona jurídica en general, como son:

(i) Los motivos estructurales, en la medida en que la organización aumenta el peligro de que las personas que por ellas actúan puedan verse tentadas a cometer el delito de *hacking* al difuminar en cierta medida su responsabilidad, sentirse arropados en su interior o bien, simplemente, para obtener una ventaja empresarial con el acceso ilícito a un sistema informático ajeno.

(ii) El factor de equilibrio entre socios-administradores en las empresas, por cuanto es posible que por el intrusismo informático la sanción penal recaiga sólo sobre el administrador, por ser quien soporta la responsabilidad por su gestión, estando expuestos los socios a poco peligro por la realización de estas conductas. Por ello, la exigencia de la responsabilidad penal a la compañía va a suponer también sanciones directas para los socios,

869 NIETO MARTÍN, A., *La responsabilidad penal de las personas jurídicas: un modelo legislativo, ed. Iustel*, Madrid, 2008, p. 37.

870 RIVAS VERDES-MONTENEGRO, C., "La responsabilidad penal de las personas jurídicas: problemas dogmáticos y soluciones legislativas", *La Ley Penal*, nº 75, ed. La Ley, Madrid, 2010, p. 2 y 3.

equiparando las exigencias que ya se establecían respecto a los administradores, con lo cual esos partícipes también se van a preocupar de un correcto funcionamiento de la empresa, tratando de evitar el *hacking*.

(iii) Reducción de costes procesales por cuanto, dentro de su ámbito de actuación, la persona moral se encuentra en mejor posición que el Estado para la prevención y persecución del intrusismo informático, más aun si atendemos al hecho de que en la mayoría de ocasiones se cometerá utilizando sus propios instrumentos o sistemas informáticos.

(iv) La causa económica, ya que exigiendo esta responsabilidad penal se trata de eliminar el beneficio que la persona jurídica pudiera obtener con el delito de *hacking*.

De esta forma, parece razonable castigar a las personas jurídicas también en este ámbito y de esta forma forzar al sector empresarial a adoptar medidas preventivas en materia de delincuencia informática, atendido el incremento y acelerado desarrollo de las nuevas tecnologías y las nuevas formas de acceso a sistemas informáticos que dificultan su persecución. Como indica MORILLAS CUEVA[871], los avances de naturaleza económica, social o tecnológica

[871] MORILLAS CUEVA, L., "La cuestión de la responsabilidad penal de

en el marco de la globalización dan lugar a novedosas formas de sociedades y con ellas también nuevas formas de cometer delitos, razón por la cual la estructura penal requiere de nuevos instrumentos en la lucha contra esta nueva delincuencia.

Con este planteamiento, procede determinar qué se entiende por "persona jurídica" en relación con las conductas que nos ocupan y delimitar quiénes deben llevar a cabo las conductas de *hacking* para que nos encontremos en los supuestos del artículo 197 *quinquies* del CP.

### *2.2 Aproximación al concepto de persona jurídica en el delito de hacking.*

Aunque no constituye el objeto del presente trabajo el concepto de las personas jurídicas ni su responsabilidad penal general, a efectos de premisa conviene tener presente que tanto la DM 2005/222/JAI en su artículo 1, como la Directiva 2013/40/UE en su artículo 2, definen a la persona jurídica de forma similar, como "*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*", si bien la Directiva cambia el término "*prerrogativas estatales*" por "*prerrogativas públicas*", matiz que en el plano teórico tiene

---

las personas jurídicas", *Anales de Derecho*, nº 29, 2011, p. 15.

trascendencia en nuestro ordenamiento, por cuanto pueden existir prerrogativas dimanantes de las Comunidades Autónomas o entidades locales, y al tratarse de prerrogativas igualmente públicas, tras la Directiva 2013/40/UE, también quedarían excluidas de la consideración de personas jurídicas. Así, si pensamos en el ejercicio de las competencias que puede asumir una Comunidad Autónoma conforme al artículo 148 CE, p.ej. en materia de Policía autonómica, o la Administración municipal o provincial según el artículo 3 del Real Decreto 2568/1986, de 28 de noviembre, por el que se aprueba el Reglamento de Organización, Funcionamiento y Régimen Jurídico de las Entidades Locales, p.ej. en la contratación de servicios de su interés, el concepto de la Directiva también excluiría a estas Administraciones de la consideración de persona jurídica, por lo que no sería posible exigir su responsabilidad penal por las conductas de intrusismo informático llevadas a cabo por sus funcionarios.

Por su parte, el legislador español no ha incluido un concepto que, obviamente, como indica DE LA CUESTA[872], deberá ser más amplio que el establecido en el artículo 297 del CP[873], referido sólo a sociedad y a los delitos societarios. En nuestro ordenamiento interno

---

872 DE LA CUESTA ARZAMENDI, J. L., "Responsabilidad penal de las personas jurídicas en el Derecho español", *Revista Peruana de Ciencias Penales*, nº 26, 2013, p. 136.

873 El artículo 297 del CP establece que "*A los efectos de este capítulo se entiende por sociedad toda cooperativa, Caja de Ahorros, mutua, entidad financiera o de crédito, fundación, sociedad mercantil o cualquier otra entidad de análoga naturaleza que para el cumplimiento de sus fines participe de modo permanente en el mercado*".

más bien se ha optado con la LO 5/2010 y con la LO 1/2015 por hacer una remisión al artículo 31 *bis* del CP, si bien tras la reforma de 2015 el precepto se ha visto desgranado en los nuevos artículos 31 *bis*, 31 *ter*, 31 *quater* y 31 *quinquies*. Ninguna de estas disposiciones establece un concepto positivo de persona jurídica, por lo que parece lógico seguir la definición contenida en los citados instrumentos internacionales que les sirven de fundamento. No obstante, el artículo 31 *quinquies* se ocupa de incluir una definición negativa para excluir a determinadas personas jurídicas del ámbito de la responsabilidad penal que podemos incluir en dos grupos:

1. Las entidades de Derecho público. En concreto, se mencionan el "*Estado, a las Administraciones públicas territoriales e institucionales, a los Organismos Reguladores" y "las organizaciones internacionales de derecho público"*.

2. Las entidades públicas empresariales y las privadas que ejercen funciones públicas, citando "*las Agencias y Entidades públicas Empresariales*" y las organizaciones "*que ejerzan potestades públicas de soberanía o administrativas*", siguiendo de esta forma el citado criterio del artículo 2 de la Directiva 2013/40/UE.

En este sentido, la FGE ha considerado en su Circular 1/2016[874] que "*Debe entenderse que el ejercicio de potestades*

[874] Circular 1/2016 de la FGE, sobre la responsabilidad penal de las personas jurídicas conforme a la reforma del Código Penal efectuada por Ley Orgánica 1/2015, p. 35, disponible en https://www.fiscal.es/fiscal/PA_WebApp_SGNTJ_NFIS/descarga/CIRCULAR

*públicas de soberanía o administrativas, por su tenor literal, resulta aplicable solo a las administraciones públicas y no a entes de naturaleza asociativa privada, como los Colegios profesionales, las Cámaras de comercio, los sindicatos o los propios partidos políticos*". Por tanto, a criterio de la FGE debe realizarse una interpretación restrictiva del precepto, posición que por otra parte resulta coherente con el principio de legalidad.

Por otra parte, estas exclusiones parecen plenamente justificadas si atendemos a que resultaría absurdo que el Estado impusiera sanciones a sus propios organismos por un delito de *hacking* llevado a cabo por sus funcionarios para así dar cumplimiento a sus fines. Tampoco constituye el objeto del presente trabajo el análisis de los fines de la pena, por lo que siguiendo a DOPICO GÓMEZ-ALLER[875], nos limitamos en este punto a señalar que el Estado no necesita sancionar a sus entidades para cumplir con sus fines de prevención general y especial[876].

---

%201-2016%20-%20PERSONAS%20JURÍDICAS.pdf?idFile=cc42d8fd-09e1-4f5b-b38a-447f4f63a041, consultado el 24 de enero de 2017.

875 DOPICO GÓMEZ-ALLER, J. "Responsabilidad de personas ...", *cit*., nota 867, p. 14.

876 En este sentido, por ser comúnmente aceptada la prevención general y especial como fines de la pena, MEZGER explicaba que "*El fin de la pena es triple: I. la pena debe actuar social-pedagógicamente sobre la colectividad (la denominada prevención general); 2. Debe proteger a la colectividad ante el sujeto que ha sido castigado y corregir a éste (la denominada prevención especial) y 3. Debe garantizar de manera justa los intereses del individuo (la denominada consideración o respeto a la personalidad)*". En este sentido, MEZGER, E., *Tratado ...*, *cit*., nota 695, p. 374.

A ello se añade que, frente a la originaria redacción del artículo 31 *bis* por la LO 5/2010, con el nuevo texto ya no quedan excluidos los "*partidos políticos y sindicatos*", derogados por la LO 7/2012[877], ni las "*sociedades mercantiles Estatales*", referencia que ha sido suprimida por la LO 1/2015.

Por tanto, al no quedar excluidos del régimen de responsabilidad penal las citadas entidades y organizaciones, se han eliminado, por una parte, las referencias a los partidos políticos y sindicatos, donde se habían dado supuestos de irregularidades en su financiación y en materia electoral. Según dispone el apartado II del Preámbulo de la LO 7/2012:

"*se modifica la regulación de la responsabilidad penal de las personas jurídicas con la finalidad de incluir a partidos políticos y sindicatos dentro del régimen general de responsabilidad, suprimiendo la referencia a los mismos que hasta ahora se contenía en la excepción regulada en el apartado 5 del artículo 31 bis del Código Penal. De este modo se supera la percepción de impunidad de estos dos actores de la vida política que trasladaba la anterior regulación, y se extiende a ellos, en los supuestos previstos por la ley, la responsabilidad por las actuaciones ilícitas desarrolladas por su*

[877] LO 7/2012, de 27 de diciembre, por la que se modifica la LO 10/1995, de 23 de noviembre, del Código Penal en materia de transparencia y lucha contra el fraude fiscal y en la Seguridad Social, publicada en el BOE de 28 de diciembre de 2012, disponible en http://www.boe.es/diario_boe/txt.php?id=BOE-A-2012-15647, consultado el 27 de enero de 2017.

*cuenta y en su beneficio, por sus representantes legales y administradores, o por los sometidos a la autoridad de los anteriores cuando no haya existido un control adecuado sobre los mismos*".

También se ha excluido a las sociedades mercantiles Estatales, cuya falta de responsabilidad penal tenía difícil justificación, por cuanto como indicaba DOPICO GÓMEZ-ALLER[878], precisamente estas sociedades por huir del régimen administrativo exigían un mayor control por parte del Estado en materia delictiva.

En consecuencia, tras la LO 1/2015 es posible la exigencia de responsabilidad penal por el delito de *hacking* a los partidos políticos, sindicatos o sociedades mercantiles Estatales. Al respecto interpreta la citada Circular 1/2016 de la FGE que la responsabilidad de los partidos políticos y sindicatos se extiende a "*a las fundaciones y entidades con personalidad jurídica a ellos vinculados*" y que los partidos políticos deben establecer programas de prevención en lo que respecta a su financiación[879].

Esta nueva inclusión de los partidos políticos, con la posibilidad de su imputación e incluso su condena con las penas del artículo 33.7, apartados b) a g)[880] al que se remite el artículo 197

878 DOPICO GÓMEZ-ALLER, J., "Responsabilidad de personas ...", *cit*., nota 867, p. 14.

879 *Vid., supra* nota 874, p. 61.

880 Como sabemos, el artículo 33.7, apartados b) a g), del CP establece: "*Las penas aplicables a las personas jurídicas, que tienen todas la consideración de graves, son las siguientes:* (...) *b) Disolución de la persona jurídica. La disolución producirá la pérdida definitiva de su personalidad*

*quinquies*, puede tener graves consecuencias, como indican CAMACHO VIZCAÍNO y CORTÉS LABADÍA[881], no sólo para el funcionamiento del partido, sino para la estructura institucional del país, en la medida en que el artículo 6 de la CE establece que "*expresan el pluralismo político, concurren a la formación y manifestación de la voluntad popular y son instrumento fundamental para la participación política*" y la Exposición de Motivos de la LO 6/2002, de 27 de junio, de Partidos Políticos dispone en su apartado I que "*forman parte esencial de la arquitectura constitucional, realizan funciones de una importancia constitucional primaria*". Por ejemplo, en la hipótesis de que fuese declarado responsable penal de un delito de *hacking* el partido político gobernante del país, porque alguno de sus representantes hubiese accedido al sistema informático de un partido de la oposición, actuando por cuenta del partido gobernante, la

---

*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. 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*".

[881] CAMACHO VIZCAÍNO, A. y CORTÉS LABADÍA, J. P., "Partidos políticos y responsabilidad penal de las personas jurídicas", *Diario La Ley on-line*, nº 8586, de 20 de julio de 2015, ed. La Ley, Madrid, p. 5.

posibilidad de que se le condenase a su disolución o los efectos en la organización parlamentaria, provocaría unas consecuencias imprevisibles a todos los niveles institucionales y dejarían de ser atendidas las citadas funciones constitucionales.

En el mismo sentido podemos entender la trascendencia que supondría para el sistema económico, político o social, las penas de disolución, suspensión de actividades o clausura previstas, entre otras, en el citado artículo 33.7 del CP si se aplicasen a los sindicatos, que también tienen declarada constitucionalmente la función de contribuir "*a la defensa y promoción de los intereses económicos y sociales que les son propios*" (artículo 7 de la CE). El hecho de que por ejemplo se disolvieran CCOO o UGT, por haber accedido por cuenta de ellos alguno de sus empleados de forma ilícita a un sistema informático, dejaría sin representación sindical a la mayoría de trabajadores del país y se dejarían de cumplir los fines constitucionales de ese sindicato.

Y otro tanto cabe decir de las sociedades mercantiles Estatales[882], en las que participa el patrimonio de la Administración

[882] La sociedad mercantil estatal se define en el artículo 111 de la Ley 40/2015, de 1 de octubre de Régimen Jurídico del Sector Público, como "*aquella sociedad mercantil sobre la que se ejerce control estatal: a) Bien porque la participación directa, en su capital social de la Administración General del Estado o alguna de las entidades que, conforme a lo dispuesto en el artículo 84, integran el sector público institucional estatal, incluidas las sociedades mercantiles estatales, sea superior al 50 por 100. Para la determinación de este porcentaje, se sumarán las participaciones correspondientes a la Administración General del Estado y a todas las*

General del Estado, por cuanto las consecuencias penales en el caso de que por su cuenta se accediese a un sistema informático ajeno se podrían traducir en pérdidas económicas para todos los ciudadanos. El hecho de que, por ejemplo, las empresas estatales Museo Nacional del Prado Difusión SA[883], Paradores de Turismo de España SA[884] o Sociedad Estatal Correos y Telégrafos SA[885], fuesen disueltas, supondría de forma inmediata, entre otros efectos, el cese en la comercialización de productos y publicaciones del Museo Nacional del Prado, en la gestión de los paradores turísticos o en un servicio tan básico como las comunicaciones a través de Correos.

En este sentido, el artículo 115 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, dispone:

"*La responsabilidad que le corresponda al empleado público como miembro del consejo de administración será directamente*

---

*entidades integradas en el sector público institucional estatal, en el caso de que en el capital social participen varias de ellas. b) Bien porque la sociedad mercantil se encuentre en el supuesto previsto en el artículo 4 de la Ley 24/1988, de 28 de julio, del Mercado de Valores respecto de la Administración General del Estado o de sus organismos públicos vinculados o dependientes*".

883 Sobre el objeto del Museo Nacional del Prado Difusión, SA: http://www.museodelpradodifusion.es/mnpd.html, consultado el 29 de enero de 2017.

884 En relación con la historia de Paradores de Turismo de España SA, http://www.parador.es/es/institucional/85-anos-de-historia, consultado el 29 de enero de 2017.

885 La información organizativa de la Sociedad Estatal Correos y Telégrafos SA se encuentra en http://www.correos.es/ss/Satellite/site/pagina-1349170529423/sidioma=es_ES, consultado el 29 de enero de 2017.

*asumida por la Administración General del Estado que lo designó*".

Esto nos lleva a plantearnos si es lógico que el Estado imponga sanciones a las empresas en las que participa con el patrimonio público. Precisamente, por la actuación de las personas que nombra y por las que responde, es decir, responder penalmente como consecuencia de la actuación de individuos que por cuenta de esas sociedades mercantiles hubieran cometido el delito de *hacking*, haciendo responsable también a la Administración General del Estado por la falta de los modelos de prevención y control que veremos en el siguiente subepígrafe. Todo ello por cuanto, siguiendo el criterio indicado de DOPICO GÓMEZ-ALLER, precisamente la finalidad de que el artículo 31 *quinquies* del CP excluya a determinadas personas jurídicas de la responsabilidad penal se encontraría en que el Estado no necesita la sanción de sus entidades para cumplir con sus fines.

Los citados inconvenientes en la condena a los partidos políticos, sindicatos o sociedades mercantiles Estatales por un delito de *hacking*, supone traer a colación los mismos motivos por los cuales habían quedado excluidos de responsabilidad penal con la LO 5/2010. Esas razones son expuestas desde dos puntos de vista, el exterior y el interior de los partidos políticos o sindicatos, por ZUGALDÍA ESPINAR[886].

[886] ZUGALDÍA ESPINAR, J. M., "La responsabilidad criminal de los partidos políticos y los sindicatos", *Revista de derecho penal y criminología*, *3.ª Época*, nº 11, enero 2014, p. 366-368.

Así, cuando actúan "hacia el exterior", lo harían para atender a sus fines constitucionales, de forma que si se exigiera su responsabilidad penal podría peligrar la división de poderes, pudiendo imponerse el "gobierno de los jueces", y se privaría a la sociedad de esas funciones que cumplen las citadas personas jurídicas.

Distinta es la actuación de estas entidades "hacia el interior", es decir, en lo relativo a su actividad interna, donde deben responder ante las distintas jurisdicciones por su gestión, razón por la cual también resulta coherente que tenga que hacerlo conforme a la normativa penal por no haber realizado un adecuado control para prevenir que sus individuos lleven a cabo un acceso ilícito a un sistema informático ajeno. De esta forma, la inclusión de su responsabilidad penal de los partidos políticos y sindicatos tras la LO 7/2012, según el apartado I de su Preámbulo "*se corresponde con el reforzamiento de la transparencia de la actividad de la administración y del régimen de responsabilidad de partidos políticos y sindicatos*".

Y estos argumentos "hacia el exterior" me parecen igualmente válidos para las sociedades mercantiles Estatales, a quienes también se asignan funciones constitucionales o de interés público, por lo que en principio puede considerarse coherente que no puedan ser castigadas por el *hacking* llevado a cabo por alguno de sus funcionarios, ya que no parece acertado que el Estado se castigue a sí mismo, o bien si atendemos al principio de división de poderes o porque el sujeto que llevase a cabo el instrusismo informático lo haría con alguna finalidad

ajena a reportar ilegalmente un beneficio al interés general. Distinta es la gestión "hacia el interior" de estas sociedades, donde también responden ante las distintas jurisdicciones y conforme a las correspondientes normativas civiles, laborales o administrativas, con ciertas peculiaridades, por lo que parece razonable que respondan, también con determinadas cautelas, cuando no se adoptan las medidas adecuadas para la prevención de las conductas delictivas que nos ocupan, cuando son cometidas por sus funcionarios. Posiblemente estos son los motivos que han llevado al legislador a introducir su responsabilidad con la reforma del año 2015. Así, precisamente por la singularidad que presentan las sociedades mercantiles Estatales es por lo que se decidió incluir con la LO 1/2015 "*el régimen de responsabilidad penal a las sociedades mercantiles estatales que ejecuten políticas públicas o presten servicios de interés económico general, a las que se podrán imponer las sanciones actualmente previstas en las letras a) y g) del apartado 7 del artículo 33 del Código Penal*" (Preámbulo III). Y el reformado artículo 31 *quinquies* CP establece en su apartado 2 que las sociedades mercantiles Estatales "*que ejecuten políticas públicas o presten servicios de interés económico general, solamente les podrán ser impuestas las penas previstas en las letras a) y g) del apartado 7 del artículo 33*", si bien, según continúa, "*Esta limitación no será aplicable cuando el juez o tribunal aprecie que se trata de una forma jurídica creada por sus promotores, fundadores, administradores o representantes con el propósito de eludir una eventual responsabilidad penal*". Es decir, la peculiaridad para las sociedades mercantiles Estatales se encuentra en

que podrá exigirse su responsabilidad penal por el intrusismo informático cuando lleven a cabo políticas públicas o servicios de interés económico general y, además, tan sólo se podrá imponer la pena de "*Multa por cuotas o proporcional*" o la "*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*", conforme al reformado artículo 31 *quinquies* y el artículo 33.7, apartados a) y g), del CP. A ello se añade que la limitación no existe en el hipotético supuesto que se apreciase que la entidad ha sido creada para acceder de forma ilícita, permanecer en sistemas informáticos ajenos de forma no autorizada o facilitar estas conductas.

En definitiva, existen determinados ámbitos que no son el hábitat natural de actuación de partidos políticos, sindicatos o sociedades mercantiles Estatales, como son las conductas encuadradas sistemáticamente entre los delitos contra la intimidad. Por ello, cuando alguno de sus miembros, representantes o funcionarios cometen un delito de *hacking*, por no tratarse propiamente de las funciones constitucionales o de interés general asignadas a estas entidades, resulta lógico que se considere responsable penalmente a estas entidades por no haber adoptado las medidas de control adecuadas para prevenirlo y evitarlo, de igual forma que resultarían responsables civil, administrativa o socialmente por el incumplimiento de esta normativa. Como indica ZUGALDÍA ESPINAR[887], cuando las citadas

[887] *Ibíd*., p. 376.

personas morales asumen el rol ajeno a sus funciones constitucional y legalmente asignadas, atribuirles un privilegio penal no tiene justificación alguna.

Con estos planteamientos, los problemas en la práctica para la exigencia de responsabilidad penal de estas personas jurídicas por el acceso ilícito, facilitar el acceso o permanecer de forma no autorizada en un sistema informático serán numerosos. QUINTERO OLIVARES[888] critica el nuevo régimen establecido respecto a partidos políticos si bien refiriéndolo a la corrupción, entre otros motivos, porque va a ser necesario diferenciar los casos de un partido político, según exista beneficio o no para el partido, y si esa ventaja es tan sólo en una zona o es extensible a todo su ámbito de actuación, así como el problema de que el sujeto esté vinculado a más de un partido. Este argumento también resulta válido para los sindicatos y las sociedades mercantiles Estatales, donde será preciso delimitar el beneficio obtenido individual o no, quién y dónde se ha obtenido. Es decir, trasladándolo al intrusismo informático, uno de los principales obstáculos con lo que en la práctica podrá encontrarse el intérprete serán los supuestos en que el delito de *hacking* se cometa por una persona que pertenece a más de un partido político o sindicato, concretando en beneficio de quién actúa y si afecta a todo el organismo o a una delegación; o si es funcionario de una sociedad mercantil Estatal, si el intrusismo se realiza en beneficio de ella o en el

888 QUINTERO OLIVARES, G., "La responsabilidad penal de los Partidos como personas jurídicas", *Actualidad Jurídica Aranzadi*, nº 859/2013, p. 5.

propio, afecta a una de las ramas de su actividad o a su funcionamiento general.

Conforme a los argumentos expuestos, podemos entender como persona jurídica a los efectos de delito de *hacking* toda entidad a la cual el derecho vigente reconoce este estatuto, salvo el Estado, otros organismos públicos que ejercen prerrogativas públicas, las organizaciones internacionales de Derecho público, las Administraciones públicas territoriales e institucionales, los Organismos Reguladores, las organizaciones internacionales de derecho público, las Agencias y Entidades públicas Empresariales y las organizaciones que ejerzan potestades públicas de soberanía o administrativas.

Por último, para que estas entidades sean responsablen de las conductas de *hacking*, es necesario que una persona física lleve a cabo la conducta del artículo 197 *bis* 1 y se cumplan los requisitos del artículo 31 *bis* 1, es decir, se ejecuten por sus representantes o por quienes estén sujetos a su autoridad, según se expone en el siguiente epígrafe.

### *2.3 Las conductas llevadas a cabo por sus representantes legales o por quienes están sometidos a su autoridad.*

Para que las conductas de *hacking* puedan entenderse cometidas por una persona jurídica, deben concurrir dos requisitos que

cita el Tribunal Supremo en su Sentencia de fecha 29 de febrero de 2016[889], "*previstos en el artículo 31 bis del Código Penal, tanto en su redacción originaria de la LO 5/2010 como en la actualmente vigente tras la reforma operada por la LO 1/2015*": en primer lugar, "*La comisión de uno de los delitos integrantes del catálogo de aquellas infracciones susceptibles de generar responsabilidad penal para la persona jurídica en cuyo seno se comete*", circunstancia que como hemos visto concurre en el citado delito conforme al artículo 197 *quinquies* del CP; y en segundo término, "*Que las personas físicas autoras de dicho delito son integrantes de la persona jurídica*".

Respecto al segundo presupuesto, en el intrusismo informático es necesario que sea llevado a cabo en beneficio de la persona jurídica por las personas físicas que cita el artículo 31 *bis*: (i) sus representantes legales o quienes están autorizados para tomar decisiones o tienen facultades de organización y control, dando lugar a lo que DEL ROSAL BLASCO denomina delitos de directivos; o (ii) quienes están sometidos a la autoridad de las personas anteriores, también conocidos como delitos de empleados[890]. O, si se prefiere, siguiendo la Circular 1/2016 de la FGE, el primer caso viene referido a una vinculación generada por "*las personas con mayores*

889 STS, Sala 2ª, de 29 de febrero de 2016, nº 154/2016, recurso 10011/2015, Pte. Excmo. Sr. D. José Manuel Maza Martín, FJ 8º.

890 La distinción entre delitos de directivos y delitos de empleados en DEL ROSAL BLASCO, B., "Responsabilidad penal de personas jurídicas: títulos de imputación y requisitos para la exención", en MORILLAS CUEVA, L. (Dir.) y VVAA, *Estudios sobre el Código penal reformado*, ed. Dykinson, Madrid, 2015, p. 85.

*responsabilidades en la entidad*", mientras que en el segundo supuesto el hecho de conexión lo crean "*las personas indebidamente controladas por aquellas*"[891]. Si bien, parece más acorde con la regulación autónoma del delito de *hacking* en el artículo 197 *quinquies* y el régimen propio de responsabilidad penal de las personas jurídicas establecido en el artículo 31 *bis* CP, entender, como ha declarado el Tribunal Supremo en su Sentencia de 16 de marzo de 2016[892], que se puede distinguir entre un delito corporativo que, como mantiene GÓMEZ-JARA DÍEZ, abarcaría lo "propio" de la responsabilidad penal de la persona jurídica[893], frente al delito individual, que comprendería la de la persona física. En concreto, la resolución establece en su FJ 5, "*Nuestro sistema, en fin, no puede acoger fórmulas de responsabilidad objetiva, en las que el hecho de uno se transfiera a la responsabilidad del otro, aunque ese otro sea un ente ficticio sometido, hasta hace bien poco, a otras formas de responsabilidad. La pena impuesta a la persona jurídica sólo puede apoyarse en la previa declaración como probado de un hecho delictivo propio*".

Esta conclusión supone posicionarse a favor de un régimen de responsabilidad propia de la persona jurídica con independencia de la

---

891 *Vid., supra* nota 868, p. 58.

892 STS, Sala 2ª, de 16 de marzo de 2016, nº 221/2016, recurso 1535/2015, Pte. Excmo. Sr. D. Manuel Marchena Gómez.

893 GÓMEZ-JARA DÍEZ, C., "Delito corporativo y responsabilidad penal de las personas jurídicas: un desarrollo coherente de la jurisprudencia del Tribunal Supremo", *Diario La Ley on-line*, nº 8830, de 23 de septiembre de 2016, ed. La Ley, Madrid, p. 1.

correspondiente a la persona física que pudiera cometer el delito de *hacking*.

Así, señala MORILLAS CUEVA[894] dos modelos de exigencia de responsabilidad penal de la persona jurídica: (i) el directo y cumulativo con la de la persona física; y (ii) el subsidiario, que tendría lugar cuando no es posible condenar al sujeto físico. Y defiende este autor el primer modelo, apoyándose tanto en el Preámbulo de la LO 5/2010[895] como en el artículo 5.3 de la Directiva 2011/36/UE[896], donde se menciona la independencia de la responsabilidad entre uno y otro tipo de persona.

Por su parte, DE LA CUESTA[897] señala (i) el modelo de responsabilidad indirecta, por el cual la exigencia a la entidad tiene su

---

894 MORILLAS CUEVA, L., "La cuestión de la responsabilidad ...", *cit*., nota 871, pp. 6 y 7.

895 Según el apartado VII del Preámbulo de la LO 5/2010, "*Se deja claro que la responsabilidad penal de la persona jurídica podrá declararse con independencia de que se pueda o no individualizar la responsabilidad penal de la persona física*".

896 El artículo 5.3 de la Directiva 2011/36/UE del Parlamento Europeo y del Consejo de 5 abril de 2011 relativa a la prevención y lucha contra la trata de seres humanos y a la protección de las víctimas y por la que se sustituye la Decisión marco 2002/629/JAI del Consejo, establece: "*La responsabilidad de las personas jurídicas en virtud de los apartados 1 y 2 se entenderá sin perjuicio de las acciones penales que puedan emprenderse contra las personas físicas que sean autores, inductores o cómplices de alguna de las infracciones contempladas en los artículos 2 y 3*". Directiva publicada en el DOUE de 15 de abril de 2011, disponible en http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2011:101:0001:0011:Es:PDF, consultado el 4 de febrero de 2017.

897 DE LA CUESTA ARZAMENDI, J. L., "Responsabilidad penal ...", *cit*., nota 872, pp. 126-128.

base en el hecho de otros, compensando los posibles excesos con la limitación de las personas que sirven de referencia e incluyendo otros requisitos de naturaleza material; (ii) el sistema de autonomía de responsabilidad, que en nuestro ordenamiento resultaría del artículo 31 *bis* 2 del CP, donde está prevista la exigencia de responsabilidad penal con independencia de que la persona física no haya sido individualizada o no se haya podido dirigir el procedimiento contra ella, tal y como se verá en el siguiente subepígrafe; y (iii) el mixto, en el que siendo independiente la responsabilidad penal de unos y otros, la de la persona jurídica se apoya en la identificación del delito cometido por la persona física, dando lugar a una mayor autorresponsabilidad con base en la falta de control. Este último sistema ha sido defendido por RIVAS VERDES-MONTENEGRO[898]. Este autor expone (i) el sistema vicarial de imputación de responsabilidad a la persona jurídica, basado en la infracción por parte del agente de la empresa, en el ejercicio de las funciones atribuidas o por cuenta de la entidad, y con la intención de un beneficio para la empresa, modelo criticado por los posibles problemas de identificación del sujeto y las pocas posibilidades de defensa de la persona jurídica; (ii) el sistema de la culpabilidad, centrado en la actuación de la persona jurídica antes y después del comportamiento del agente, pudiendo quedar exenta de responsabilidad si ha adoptado las medas adecuadas de prevención y descubrimiento del delito; y (iii) el citado sistema mixto, por el que se imputa la responsabilidad a la

[898] RIVAS VERDES-MONTENEGRO, C. ,"La responsabilidad penal ...", *cit*., nota 870, p. 4, 5 y 8.

persona moral por la actuación de la persona física (como en el vicarial) pero desde ese momento se considera la actuación de la entidad (como en el de culpabilidad), para concretar con agravantes y atenuantes la sanción.

Para el Tribunal Supremo, en la mencionada Sentencia de 16 de marzo de 2016, no es posible un sistema penal de transferencia de la responsabilidad, donde la responsabilidad de la persona jurídica descanse sobre el hecho ajeno, lo que me parece coherente con los principios informadores del Derecho penal, como son el principio del hecho y el de culpabilidad. Esta conclusión resulta de la citada regulación propia de la responsabilidad penal de la persona jurídica en el delito de intrusismo informático. Frente a esta postura, la citada Sentencia rechaza el criterio de la Circular 1/2016 de la FGE, donde se considera que estamos ante un sistema de responsabilidad penal vicarial o por representación, donde es necesaria "*la previa comisión de un delito por una persona física en las concretas circunstancias que se establecen*" y una conexión entre la persona física y la jurídica[899].

Lo expuesto no significa, tal y como se viene anticipando, que la responsabilidad de la entidad aparezca totalmente desvinculada del acceso ilícito, facilitar estas conductas o la permanencia no autorizada en el sistema, llevado a cabo por sus empleados o representantes, que se convierte en delito de referencia. Es decir, desde un punto de vista estructural habrá que comprobar si la persona jurídica ha adoptado las

899 *Vid., supra* nota 874, p. 58.

medidas de prevención y control que veremos en el siguiente subepígrafe. Así, como concluye la citada STS de 16 de marzo de 2016:

"*El hecho sobre el que ha de hacerse descansar la imputación no podrá prescindir, claro es, del delito de referencia atribuido a la persona física. Pero habrá de centrarse en su averiguación desde una perspectiva estructural. Se tratará, por tanto, de una indagación sobre aquellos elementos organizativo-estructurales que han posibilitado un déficit de los mecanismos de control y gestión, con influencia decisiva en la relajación de los sistemas preventivos llamados a evitar la criminalidad en la empresa. La responsabilidad de la persona jurídica ha de hacerse descansar en un delito corporativo construido a partir de la comisión de un previo delito por la persona física, pero que exige algo más, la proclamación de un hecho propio con arreglo a criterios de imputación diferenciados y adaptados a la especificidad de la persona colectiva. De lo que se trata, en fin, es de aceptar que sólo a partir de una indagación por el Juez instructor de la efectiva operatividad de los elementos estructurales y organizativos asociados a los modelos de prevención, podrá construirse un sistema respetuoso con el principio de culpabilidad*".

Más concretamente, para que el citado delito pueda entenderse cometido por una persona jurídica, es necesario que sean llevadas a cabo en su propio beneficio por las personas físicas que cita el artículo 31 *bis*: (i) sus representantes legales o quienes están autorizados para

tomar decisiones o tienen facultades de organización y control, dando lugar a lo que DEL ROSAL BLASCO denomina delitos de directivos; o (ii) quienes están sometidos a la autoridad de las personas anteriores, también conocidos como delitos de empleados[900].

Así pues, analizando los dos supuestos contemplados en los apartados a) y b) mencionado precepto, partiendo en ambos casos de que "*En los supuestos previstos en este Código, las personas jurídicas serán penalmente responsables*" "*De los delitos cometidos en nombre o por cuenta de las mismas, y en su beneficio directo o indirecto*":

1) En el primer caso, el artículo 31 *bis* ha omitido la referencia a los administradores de hecho o derecho introducida por la LO 5/2010 y se ha optado por una descripción más detallada, de tal forma que deben ser "*sus representantes legales o por aquellos que actuando individualmente o como integrantes de un órgano de la persona jurídica están autorizados para tomar decisiones en nombre de la persona jurídica u ostentan facultades de organización y control dentro de la misma*".

Se trata, como indica PORRES ORTIZ DE URBINA[901], de la responsabilidad penal de la persona jurídica por los actos de directivos. De tal forma que en el delito de intrusismo informático es preciso, siguiendo el planteamiento general de este autor, que: (i) el

[900] La distinción entre delitos de directivos y delitos de empleados en DEL ROSAL BLASCO, B., "Responsabilidad penal ...", *cit*., nota 890, p. 85.

[901] PORRES ORTIZ DE URBINA, E., "Responsabilidad penal de las personas jurídicas", *Revista de Jurisprudencia El Derecho*, nº 2, ed. El Derecho, 1 de junio de 2015, p. 5.

directivo lleve a cabo el acceso ilícito al sistema informático en nombre o por cuenta de la persona jurídica, es decir, dentro del contenido formal y material del mandato y representación quedando excluido el caso en el que el sujeto se extralimite. Esto implica que el acceso se realizaría, conforme analiza DOPICO GÓMEZ-ALLER[902] en el marco de las funciones empresariales, desviándose del correcto ejercicio de las funciones y actuando por la persona jurídica; y (ii) que lo haga en beneficio de esa entidad, término que comprende cualquier beneficio o ventaja, como podría ser tomar el control de los sistemas informáticos de la competencia de una empresa, y sustituye al anterior "en provecho", que daba lugar a numerosas interpretaciones. Puede ser un beneficio directo o empresarial, o indirecto o ahorro en costes a través de la conducta delictiva, lo que excluye la comisión del delito de *hacking* por estas personas físicas cuando su realización no tienen relación con la persona jurídica.

El término representante legal deberá interpretarse restrictivamente y en consecuencia considerar como tal a las personas cuya representación se extiende a todos los actos comprendidos en el objeto social delimitado en los estatutos de conformidad con los artículos 233 y 234 del Real Decreto Legislativo 1/2010, de 2 de julio, por el que se aprueba el texto refundido de la Ley de Sociedades de Capital, y pueden ser tanto representantes orgánicos como no orgánicos de la persona jurídica en un sentido legal, dentro de las

902 DOPICO GÓMEZ-ALLER, J., "Responsabilidad de personas ...", *cit*., nota 867, p. 18.

facultades que se les han atribuido[903], mientras que los que actúan individualmente o como integrantes de un órgano de la persona jurídica deberán estar autorizados para tomar decisiones en nombre de la persona jurídica o tener facultades para su organización y control.

2) En el segundo de los casos, el delito sería cometido por una persona sujeta a la autoridad de las personas físicas citadas en el primer caso, es decir, empleando los términos del artículo 31 *bis*, "*por quienes, estando sometidos a la autoridad de las personas físicas mencionadas en el párrafo anterior, han podido realizar los hechos por haberse incumplido gravemente por aquéllos los deberes de supervisión, vigilancia y control de su actividad atendidas las concretas circunstancias del caso*".

En este supuesto, se trata de una falta de control debido sobre la persona dependiente, que como indica ORTIZ DE URBINA[904] no supone que todo incumplimiento de esos deberes conlleva la responsabilidad de la persona jurídica, sino tan sólo el grave, lo que supone analizar cada caso particular y verificar si se habían asumido medidas de prevención y represión ante un posible intrusismo informático. De esta forma, se complica la responsabilidad penal en estos casos, ya que siguiendo a este autor, se hace preciso acudir a la

---

903 Si sólo se considerasen representantes legales los orgánicos, supondría una interpretación excesivamente restrictiva del precepto, por ejemplo se excluiría el caso del apoderado de la persona jurídica. En este sentido, DEL ROSAL BLASCO, B., "Responsabilidad penal ...", *cit*., nota 890, p. 91.

904 PORRES ORTIZ DE URBINA, E., "Responsabilidad penal ...", *cit*., nota 901, pp. 6 y 7.

normativa extrapenal para delimitar las obligaciones personales de control que tienen atribuidas las personas físicas para que no se lleve a cabo el *hacking*. En este sentido, el Consejo de Estado, en su Informe a la futura LO 1/2015 manifestaba la necesidad de una reforma inmediata en la legislación mercantil para regular esas funciones de vigilancia y control en los siguientes términos: "*el principio de seguridad jurídica impone un determinado nivel de certeza en torno a los medios, órganos y cauces exigibles para el desarrollo de esas funciones de vigilancia y control, aspectos cuya regulación corresponde, por su propia naturaleza, a la legislación mercantil o a la que resulte de aplicación a las personas jurídicas de que en cada caso se trate*"[905].

Por otra parte concurre una cierta contradicción, ya que si el fundamento de estos casos se ubica en la omisión de diligencia de los directivos hacia los empleados, no resulta coherente que se afirme que la persona jurídica quede exenta si ha existido un sistema adecuado de prevención, sin establecer condiciones adicionales como en el caso de los directivos.

Por último, en este segundo grupo la conducta se debe llevar a cabo "*en el ejercicio de actividades sociales*", lo que supone una desviación de su correcto ejercicio, y *"por cuenta y en beneficio directo o indirecto de las mismas*", elemento al que ya nos hemos

[905] Dictamen del Consejo de Estado de fecha 27 de junio de 2013, disponible en http://www.boe.es/buscar/doc.php?id=CE-D-2013-358, consultado el 4 de febrero de 2017.

referido en relación con las conductas llevadas a cabo por los representantes de la persona jurídica.

### *2.4 La exigencia de responsabilidad penal a la persona jurídica por el delito de hacking.*

Por último, el legislador ha regulado la responsabilidad de la persona jurídica aun cuando no fuese posible individualizar a la persona física que ha cometido el delito de *hacking*, y con independencia de la culpabilidad de estas personas o que hayan fallecido o hayan eludido su enjuiciamiento. Así, según lo establecido en el artículo 31 *ter* del CP:

"*1. La responsabilidad penal de las personas jurídicas será exigible siempre que se constate la comisión de un delito que haya tenido que cometerse por quien ostente los cargos o funciones aludidas en el artículo anterior, aun cuando la concreta persona física responsable no haya sido individualizada o no haya sido posible dirigir el procedimiento contra ella. Cuando como consecuencia de los mismos hechos se impusiere a ambas la pena de multa, los jueces o tribunales modularán las respectivas cuantías, de modo que la suma resultante no sea desproporcionada en relación con la gravedad de aquéllos. 2. La concurrencia, en las personas que materialmente hayan realizado los hechos o en las que los hubiesen hecho posibles por no haber ejercido el debido control, de circunstancias que afecten*

*a la culpabilidad del acusado o agraven su responsabilidad, o el hecho de que dichas personas hayan fallecido o se hubieren sustraído a la acción de la justicia, no excluirá ni modificará la responsabilidad penal de las personas jurídicas, sin perjuicio de lo que se dispone en el artículo siguiente".*

De esta forma, como indica BACIGALUPO SEGGESE, la responsabilidad penal de la persona jurídica no depende de la responsabilidad penal de la persona física, sino de que exista un hecho de conexión que se atribuya a la persona física[906]. Es decir, los vínculos de conexión a los que se ha hecho referencia en este epígrafe.

Por otra parte, esta previsión es adecuada en el difícil ámbito de lucha contra la criminalidad informática. Castigar a la persona jurídica con independencia de la falta de individualización del delito en persona física concreta supone, desde mi punto de vista, un fortalecimiento de las medidas de presión sobre la persona jurídica en cuanto a la adopción de medios para tratar de evitar la comisión del delito de intrusismo informático y, a su vez, obstaculizar obras de ingeniería procesal o que por parte de los encargados o representantes de la persona jurídica se trate de esconder o ayudar al infractor para de esta forma dificultar a su vez el enjuiciamiento de estas entidades. Es decir, estamos ante una medida más, dirigida a facilitar la prevención y persecución de estos delitos, ya de por sí complejos.

---

906 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)", *Diario La Ley on-line*, nº 7541, de 5 de enero de 2011, ed. La Ley, Madrid, p. 4.

Con las citadas premisas, en el caso de las personas jurídicas es preciso el mismo respeto de los derechos y garantías constitucionales y principios que informan el Derecho penal, que como ha declarado el Tribunal Supremo en la citada Sentencia de 29 de febrero de 2016 "*ampararían también a la persona jurídica de igual forma que lo hacen en el caso de las personas físicas cuyas conductas son objeto del procedimiento penal*"[907].

Además, cuando se produzca el acceso ilícito a todo o parte de un sistema informático, o se facilite, o se permanezca de forma no autorizada, por los representantes legales de una persona jurídica, o bien por las personas físicas que estén autorizadas para tomar decisiones o tienen facultades de organización y control, o por quienes estén sometidos a la autoridad de las personas anteriores, siguiendo la mencionada resolución, será necesario como presupuesto "*la exigencia del establecimiento y correcta aplicación de medidas de control eficaces que prevengan e intenten evitar, en lo posible, la comisión de infracciones delictivas por quienes integran la organización*", es decir, "*ha de establecerse a partir del análisis acerca de si el delito cometido por la persona física en el seno de aquella ha sido posible, o facilitado, por la ausencia de una cultura de respeto al Derecho, como fuente de inspiración de la actuación de su estructura organizativa e independiente de la de cada una de las personas físicas que la integran, que habría de manifestarse en alguna clase de formas concretas de vigilancia y control del*

907 STS de 29 de febrero de 2016, *cit*., nota 889, FJ 8º.

*comportamiento de sus directivos y subordinados jerárquicos, tendentes a la evitación de la comisión por éstos de los delitos enumerados en el Libro II del Código Penal como posibles antecedentes de esa responsabilidad de la persona jurídica*".

De esta forma, como se ha apuntado anteriormente, el legislador ha optado por hacer partícipe en la prevención de estos delitos a la propia persona jurídica, por cuanto va a poder eludir su responsabilidad adoptando las medidas que se establecen en el artículo 31 *bis*, apartados 2 y 5 del CP. En concreto, está prevista la exención de responsabilidad de la persona jurídica cuando concurran las siguientes condiciones:

1ª Que "*el órgano de administración ha adoptado y ejecutado con eficacia, antes de la comisión del delito, modelos de organización y gestión que incluyen las medidas de vigilancia y control idóneas para prevenir delitos de la misma naturaleza o para reducir de forma significativa el riesgo de su comisión*".

Además, en relación con este primer requisito, el legislador exige en el apartado 5 del mencionado artículo 31 *bis*, que esos modelos deben cumplir a su vez una serie de requisitos: "*Identificarán las actividades en cuyo ámbito puedan ser cometidos los delitos que deben ser prevenidos*", "*Establecerán los protocolos o procedimientos que concreten el proceso de formación de la voluntad de la persona jurídica, de adopción de decisiones y de ejecución de las mismas con relación a aquéllos*", "*Dispondrán de modelos de gestión de los recursos financieros adecuados para impedir la comisión de los*

*delitos que deben ser prevenidos*", "*Impondrán la obligación de informar de posibles riesgos e incumplimientos al organismo encargado de vigilar el funcionamiento y observancia del modelo de prevención*", "*Establecerán un sistema disciplinario que sancione adecuadamente el incumplimiento de las medidas que establezca el modelo*" y "*Realizarán una verificación periódica del modelo y de su eventual modificación cuando se pongan de manifiesto infracciones relevantes de sus disposiciones, o cuando se produzcan cambios en la organización, en la estructura de control o en la actividad desarrollada que los hagan necesarios*".

Al respecto, pensemos en una empresa de servicios informáticos, donde sus empleados cuentan con numerosos recursos técnicos para el acceso remoto a los sistemas informáticos de clientes y esta circunstancia es aprovechada por alguno de sus representantes o trabajadores para cometer el delito de *hacking*. En estos casos, para que la persona jurídica no fuese responsable conforme al artículo 197 *quinquies* del CP debería haber existido con anterioridad a la comisión del delito un sistema de medidas de prevención y control eficaces para impedir ese delito, adoptadas por su administrador o consejo de administración. Por ejemplo, estableciendo un protocolo que exija la identificación de la persona física para el acceso y la previa autorización del cliente para llevar a cabo esa entrada en concreto en su sistema. Además, ese protocolo debería identificar la posible comisión del delito de *hacking*, el consentimiento a su vez que tiene la persona física para actuar por cuenta de la persona jurídica, debería

estar debidamente financiado para hacer posible su funcionamiento, se tendría que dar cuenta de su funcionamiento y riesgos al órgano de control de su cumplimiento, incluiría un régimen disciplinario en caso de no respetarse su contenido y, por último, debería verificarse en caso de que se produjese un caso de *hacking* o existieran cambios en la estructura u organización de la persona jurídica.

2ª El requisito de que "*la supervisión del funcionamiento y del cumplimiento del modelo de prevención implantado ha sido confiada a un órgano de la persona jurídica con poderes autónomos de iniciativa y de control o que tenga encomendada legalmente la función de supervisar la eficacia de los controles internos de la persona jurídica*".

Por tanto, en el ejemplo citado también sería preciso que el citado protocolo o las medidas que se hubiesen adoptado por la empresa para prevenir el delito específico del intrusismo informático sean supervisados por un órgano autónomo de control de la persona jurídica o que tuviese esa función de vigilancia por imperativo legal. Así, según establece el artículo 31 *bis*, apartado 3, "*En las personas jurídicas de pequeñas dimensiones, las funciones de supervisión a que se refiere la condición 2.ª del apartado 2 podrán ser asumidas directamente por el órgano de administración. A estos efectos, son personas jurídicas de pequeñas dimensiones aquéllas que, según la legislación aplicable, estén autorizadas a presentar cuenta de pérdidas y ganancias abreviada*".

3ª Además de los citados modelos y su control, "*los autores individuales han cometido el delito eludiendo fraudulentamente los modelos de organización y de prevención*", es decir, no se suficiente con que la persona jurídica haya adoptado todas las medidas exigidas para la prevención y control del acceso ilícito a un sistema informático ajeno por parte de las personas físicas que actúan por cuenta de ella, sino que para quedar exenta de responsabilidad también es necesario que los autores individuales hayan burlado esas medidas de forma fraudulenta. Así, en el ejemplo mencionado, el empleado o encargado en la estructura de la empresa, aprovechando los medios técnicos a su alcance, comete el delito de *hacking* y lo hace sin respetar el protocolo de identificación y consentimiento del cliente implantado por la empresa para de esta forma acceder a ese sistema informático ajeno.

4ª En último lugar, a las citadas medidas de prevención, control y vulneración de esos modelos, se exige un plus de control por la persona jurídica, es decir, que "*no se ha producido una omisión o un ejercicio insuficiente de sus funciones de supervisión, vigilancia y control por parte del órgano al que se refiere la condición 2.ª*", circunstancia que deberá valorarse en cada caso, atribuyendo al juzgador la función de decidir cuándo es o no suficiente la función de supervisión, vigilancia o control de la persona jurídica en el caso concreto. Habría sido deseable una mayor concreción del legislador en esta condición, a efectos de no tirar por la borda un riguroso cumplimiento de todos los requisitos anteriores por una persona jurídica por la puntual interpretación del precepto que pueda realizar

un órgano jurisdiccional.

En cualquier caso, según concluye el artículo 31 *bis*, apartado 2, "*En los casos en los que las anteriores circunstancias solamente puedan ser objeto de acreditación parcial, esta circunstancia será valorada a los efectos de atenuación de la pena*".

Por último, se ha discutido la naturaleza de esta exención de responsabilidad de la persona jurídica. Para BACIGALUPO SAGGESSE[908] el modelo de imputación debe basarse en que exista el hecho de conexión y en la idea de la culpabilidad por el defecto de organización.

Sin embargo, la FGE ha considerado en su Circular 1/2016[909] respecto de la exención de responsabilidad penal del artículo 31 *bis* del CP que en principio podría considerarse un supuesto de falta de tipicidad, por cuanto si se parte de una mala organización para exigir la responsabilidad penal de la persona jurídica, en el caso de que exista un plan diligente de prevención, supone que desaparece el elemento del tipo, ya sea en su parte subjetiva o en su parte objetiva. No estaríamos en el caso de una eximente, que nos remite a una conducta antijurídica o entender que la persona jurídica no le fuera imputable la conducta, sino que al existir unas medidas anteriores a la comisión del delito, faltaría el elemento básico del hecho típico (tipo

908 BACIGALUPO SAGGESSE, S., "Artículo 31 y 31 *bis*", en GÓMEZ TOMILLO, M. (Dir.) y VVAA, *Comentarios al Código Penal*, ed. Lex Nova, primera edición, Valladolid, 2010, p. 273.

909 *Vid., supra* nota 874, p. 55 y 56.

objetivo) o, en todo caso, un elemento del tipo subjetivo, dolo o culpa (tipicidad subjetiva).

Sin embargo, para la FGE puesto que, según su postura, el sistema establecido por el legislador es de responsabilidad indirecta o vicarial en la medida en que la responsabilidad de la persona jurídica se basa en el hecho ajeno, la comisión del delito por la persona física va a determinar la responsabilidad de la persona jurídica, que no obstante va a quedar exenta probando la existencia del modelo de prevención y control. Por ello, atendido el sistema establecido en el artículo 31 *bis* del CP, para la Fiscalía estamos ante un supuesto de exclusión personal de punibilidad. Así, "*concurrentes en el momento en el que la persona física comete el delito y transfiere la responsabilidad a la persona jurídica, los modelos de organización que cumplen los presupuestos legales operarán a modo de excusa absolutoria, como una causa de exclusión personal de la punibilidad y no de supresión de la punibilidad, reservadas estas últimas causas para comportamientos post delictivos o de rectificación positiva, como los contemplados en las circunstancias atenuantes del art. 31 quater*".

Por su parte, el Tribunal Supremo en el FJ 8º de la mencionada Sentencia de 29 de febrero de 2016 ha mantenido distinto criterio al de la FGE. En concreto, el Tribunal ha destacado la discutible naturaleza de la eximente, "*en cuanto relacionada con la exclusión de la culpabilidad, lo que parece incorrecto, con la concurrencia de una causa de justificación o, más bien, con el tipo objetivo, lo que sería*

*quizá lo más adecuado puesto que la exoneración se basa en la prueba de la existencia de herramientas de control idóneas y eficaces cuya ausencia integraría, por el contrario, el núcleo típico de la responsabilidad penal de la persona jurídica, complementario de la comisión del ilícito por la persona física*".

Así, en la citada Sentencia se considera que la eximente tiene una naturaleza que se correspondería con la falta de tipicidad y de paso se rebate, en el mismo Fundamento, la conclusión de la Circular 1/2016, porque "*una <<excusa absolutoria>> ha de partir, por su propia esencia, de la previa afirmación de la existencia de la responsabilidad, cuya punición se excluye, mientras que a nuestro juicio la presencia de adecuados mecanismos de control lo que supone es la inexistencia misma de la infracción. Circunstancia de exención de responsabilidad que, en definitiva, lo que persigue esencialmente no es otra cosa que posibilitar la pronta exoneración de esa responsabilidad de la persona jurídica, en evitación de mayores daños reputacionales para la entidad, pero que en cualquier caso no debe confundirse con el núcleo básico de la responsabilidad de la persona jurídica, cuya acreditación por ello habrá de corresponder a la acusación, en caso de no tomar la iniciativa la propia persona jurídica de la búsqueda inmediata de la exención corriendo con la carga de su acreditación como tal eximente*". Este criterio también ha sido defendido por DE LA CUESTA[910], quien

[910] DE LA CUESTA ARZAMENDI, J. L., "Responsabilidad penal ...", *cit*., nota 872, pp. 118, 129 y 130.

considera que, partiendo de la capacidad general de autoorganización de la persona jurídica, estamos ante un supuesto de falta de tipicidad respecto del resultado imprevisible o inevitable. Así, según este autor, en lugar de la culpabilidad, mejor se debe elaborar el núcleo de injusto de la persona moral sobre la vulneración de su posición de garante, es decir, su deber de autoorganización adecuada para evitar el delito en el marco de las actividades realizadas por su cuenta y beneficio. De esta forma, la responsabilidad penal de la persona jurídica por el delito de *hacking* surgiría cuando a la infracción del deber de adoptar medidas de prevención y control se pueda imputar objetivamente la comisión de ese delito por parte de alguna de las personas físicas que cita el precepto.

Desde mi punto de vista, esta última postura de la naturaleza de la exención de responsabilidad de la persona jurídica como carente de tipicidad parece la más acertada. No entiendo que estemos ante un supuesto de falta de culpabilidad de la persona jurídica por el hecho de que adopte las medidas adecuadas para impedir el delito de *hacking* y aun así se haya cometido por alguno de sus agentes. Así, considerando desde el punto de vista del juicio de reproche que, según MEZGER, la culpabilidad es "*una determinada situación de hecho, de ordinario psicológica (situación de hecho de la culpabilidad), en la que se conecta el reproche contra el autor y, consiguientemente, la pena que al autor ha de aplicarse*"[911], no parece que la posición que defiende la naturaleza de la exclusión de responsabilidad en un supuesto de falta

[911] MEZGER, E., *Tratado de Derecho Penal ..., cit*., nota 695, p. 9.

de culpabilidad sea lo más ajustado a la previsión del artículo 31 *bis* CP, porque ello obligaría al correspondiente juicio de reprochabilidad con todos los matices e inconvenientes que todo juicio conlleva. Más bien, si consideramos la tipicidad como entendía VON LISZT, es decir, "*aquel acto que corresponde a uno de los hechos exactamente circunscritos y exclusivamente enumerados en la ley*"[912] o según expone MEZGER como "*el injusto descrito concretamente por la ley en sus diversos artículos y a cuya realización va ligada la sanción penal*"[913], en el caso del intrusismo informático *a priori* no hay duda en cuanto al punto de partida, relativo a la inexistencia de un sistema de prevención y control por parte de la persona jurídica para la comisión del delito de *hacking* por parte de sus empleados o representantes. De tal forma que, sin ese presupuesto inicial, es decir, si existe un adecuado sistema de prevención y control y la persona física que actúa por la persona jurídica lo burla fraudulentamente, no va a existir responsabilidad penal para ésta última. Por ello, considero que, en lugar de una falta de reproche hacia la persona jurídica que obligaría al correspondiente juicio de valor con los problemas que ello entrañaría, en estos casos faltará el elemento básico de la tipicidad de la conducta. Este planteamiento además contribuye a eludir una consideración inicial de responsabilidad de la persona jurídica desde el principio, imponiéndole la carga de la prueba de su propia inocencia en el procedimiento que condujese a la exclusión de la punibilidad, que sería la postura que plantea la FGE. Esta naturaleza expuesta en

912 VON LISZT, F., *Tratado de Derecho Penal* ..., *cit*., nota 335, p. 444.

913 MEZGER, E., *Tratado de Derecho Penal* ..., *cit*., nota 341, p. 300.

su Circular 1/2016, considerando estos supuestos como excusas absolutorias vinculadas a la punibilidad, partiría de la previa afirmación de la responsabilidad de la persona jurídica que se excluiría por la falta de punibilidad. Sin embargo, si atendemos a la definición de las condiciones de punibilidad como una serie de casos en los que el legislador ha hecho depender la efectividad de la sanción penal de la existencia de circunstancias externas, independientes del acto punible mismo y que se añaden a él[914], resulta obvio que la autoorganización de la persona jurídica no es una circunstancia externa, sino una medida adoptada por la entidad que determina su exclusión de responsabilidad. Por ello entiendo, siguiendo el criterio del Tribunal Supremo, que la existencia de las medidas de prevención y control precisamente lo que evidenciarían es la falta de responsabilidad de la entidad en el acceso ilícito a un sistema informático ajeno, evitando así un juicio *ab initio* a la propia persona jurídica por el simple hecho de que alguno de sus empleados cometiesen el delito de *hacking* e impondría a la acusación la carga de la prueba de que las medidas no se han adoptado conforme exige el artículo 31 *bis* del CP para poder proceder también contra la persona moral por ese delito, lo que resulta más acorde con el principio acusatorio del procedimiento penal y el derecho fundamental a la presunción de inocencia declarado en el artículo 24.2 de la CE.

914 VON LISZT, F., *Tratado de Derecho Penal ..., cit*., nota 697, p. 445.

*3. TOMA DE POSICIÓN.*

La regulación de la responsabilidad de la persona jurídica en el artículo 197 *quinquies*, por los delitos de *hacking* que se llevan a cabo en su nombre o ejercicio de actividades sociales y por cuenta y beneficio de la persona jurídica, no plantean problemas desde el plano teórico sin perjuicio de todos los que supone el nuevo artículo 31 *bis* para la parte general del Derecho penal, algunos de los cuales se han apuntado en el presente Capítulo.

De este último artículo resulta la responsabilidad penal de la persona jurídica por el acceso ilícito a sistemas informáticos llevados a cabo bien por sus representantes o autorizados, o bien por las personas sometidas a la autoridad de ellos.

De esta forma, con la introducción de la responsabilidad penal de las personas morales en el intrusismo informático se emplea un nuevo instrumento para la prevención y la persecución de estos delitos, que ya de por sí son suficientemente complejos pero que además están en continua evolución, mostrándose el Estado en cierta medida ineficaz *per se* para castigarlos y necesitando por ello del empleo de nuevos mecanismos para asegurar que estas conductas no queden impunes.

Así, en el caso del *hacking* cobra especial interés la exigencia de responsabilidad si atendemos a los motivos que se han expuesto en el epígrafe 2 de este Capítulo, es decir, estructurales para que no se

difuminen responsabilidades, de equilibrio en las responsabilidades, reducción de costes en su persecución o económicos para eliminar beneficios ilícitamente obtenidos.

De todo ello resulta, según considero, que el castigo penal a la persona jurídica por el acceso ilícito a sistemas informáticos ajenos está justificado.

En cuanto al concepto de persona jurídica como punto de partida, entiendo que ante la falta de una definición positiva por el legislador español, hay que acudir a los instrumentos internacionales y a la delimitación negativa del artículo 31 *quinquies* CP. De esta forma resulta que, conforme al artículo 2 de la Directiva 2013/40/UE y el citado precepto, quedaría comprendido en los casos de responsabilidad criminal por el delito de *hacking* toda entidad a la cual el derecho vigente reconoce este estatuto, salvo el Estado, otros organismos públicos que ejercen prerrogativas públicas, las organizaciones internacionales de Derecho público, las Administraciones públicas territoriales e institucionales, los Organismos Reguladores, las organizaciones internacionales de Derecho público, las Agencias y Entidades públicas Empresariales y las organizaciones que ejerzan potestades públicas de soberanía o administrativas. Por exigirlo así el principio de legalidad entiendo que la interpretación debe realizarse de forma restrictiva.

Por otra parte, las citadas exclusiones me parecen justificadas si consideramos que resultaría absurdo que el Estado castigara a sus

propios organismos por el delito de *hacking* realizado por sus funcionarios.

Como se ha expuesto, el nuevo régimen ya no excluye a los partidos políticos, sindicatos ni sociedades mercantiles Estatales, lo cual resulta razonable por cuanto, aunque entendamos que tienen asignadas determinadas funciones constitucionales o de interés general, el intrusismo informático no se presenta entre ellas, razón por la cual resulta lógica la exigencia de la responsabilidad penal "hacia el interior", es decir, contemplada desde el punto de vista de no haber adoptados las medidas de prevención y control para impedirlo. Si la persona jurídica responde civil, administrativa o laboralmente por la vulneración de esa normativa en cada caso, no se entiende que no deba responder también en el ámbito penal cuando se den los presupuestos para ello. Además, no concurre justificación alguna para que los partidos políticos o sindicatos tengan el privilegio de no asumir responsabilidad penal por el *hacking* llevado a cabo por sus agentes, por cuenta de la persona moral y en beneficio de ésta.

Todo ello no significa que sea sencilla la exigencia de esa responsabilidad penal, por cuanto restará por delimitar qué persona física ha cometido el acceso ilícito al sistema informático ajeno, o lo ha facilitado o se ha mantenido en el sistema sin autorización, en qué ámbito, o si afecta a toda la extensión de la persona jurídica, entre otros factores de difícil delimitación.

Por otra parte, en el artículo 31 *bis* se distingue entre lo que se denominan delitos de directivos y delitos de empleados. Al respecto se

plantea la dependencia o independencia entre la responsabilidad individual del sujeto y la de la persona moral, y entiendo que en nuestro ordenamiento el sistema introducido es el de responsabilidad directa de la persona jurídica, de forma autónoma de la persona física, por cuanto el propio artículo 31 *bis* 2 del CP se encarga de diferenciarlos y de establecer la responsabilidad con independencia de que la persona física no sea castigada por el delito.

En el caso de los directivos, deberán llevar a cabo el intrusismo informático dentro de su mandato o representación, no comprendiendo las actuaciones fuera de ese ámbito, lo que excluye los casos de extralimitación, y además en beneficio de la entidad.

Por lo que respecta al delito de *hacking* cometido por personas sujetas a la autoridad de esos directivos, deberá existir un incumplimiento grave de los deberes de supervisión, vigilancia y control, lo que exigirá el análisis caso por caso y acudir a la normativa extrapenal para delimitar esas obligaciones en materia de acceso a sistemas informáticos. Además, la previsión puede plantear problemas interpretativos en la medida en que se exige que se hayan incumplido los deberes de supervisión, vigilancia y control y a la vez está prevista la exención de responsabilidad penal de la persona jurídica si ha existido un sistema adecuado de prevención.

En cuanto a la pena, para que se pueda castigar a la persona moral en el delito de *hacking* es preciso un hecho de conexión con el sujeto que lo ha cometido. Esa sanción con independencia de la responsabilidad penal de la persona física me parece una herramienta

adecuada para disuadir a las entidades en la comisión de estos delitos y para que adopten las medidas dirigidas a prevenirlos.

A partir del artículo 31 *bis* del CP, entiendo que el modelo adoptado por el legislador de exención de responsabilidad penal para la persona jurídica, derivada del delito de intrusismo informático, descansa sobre la falta de tipicidad que existe en los casos en los que se han adoptado los medios necesarios para impedir el delito. De esta forma, la falta de tipicidad de estas conductas cuando concurren los elementos de exención de responsabilidad penal determina que no sea la persona jurídica quien deba concurrir al juicio para determinar si ha adoptado las medidas adecuadas o no. Por el contrario, desde el inicio podrá comprobarse que falta la tipicidad, posibilitando así la pronta exoneración de esa responsabilidad. Si existe un adecuado sistema de prevención y control y la persona física que actúa por la persona jurídica lo burla fraudulentamente, no va a existir responsabilidad penal para ésta última por faltar la tipicidad en la conducta de la persona moral.

En definitiva, aunque la reforma por la que se introduce la responsabilidad de las personas jurídicas ha sido considerada la reforma más importante introducida en nuestros Códigos penales[915], todavía no tenemos constancia de sentencias que hayan resuelto sobre la responsabilidad penal de las personas jurídicas por el delito de *hacking* aplicando el artículo 197 *quinquies*, y las resoluciones en las

915 DEL ROSAL BLASCO, B., "Responsabilidad penal …", *cit*., nota 890, p. 82.

que se ha resuelto sobre la responsabilidad de las personas jurídicas por otros delitos son muy escasas[916], por lo que no resulta posible delimitar *a priori* el alcance práctico de la reforma en este ámbito.

[916] En este sentido, la SAP de Barcelona nº 155/2014, Seccion 8ª, de 19 de febrero de 2014, Pte. Ilmo. Sr. D. Jesús María Barrientos Pacho (JUR 2014\84549), que condenaba a la mercantil GENTLE HOSTELERY ASSOCIATE, SL, como responsable penal y civilmente de un delito contra el medio ambiente de los artículos 325.1, *in fine*, y 326 b y d del Código Penal, con la concurrencia de la atenuante muy cualificada de reparación del daño, a la pena de multa de dos años con una cuota también de seis euros por cada una de las cuotas, además de condenar también a la persona física que realizó la conducta "*personalmente y bajo el paraguas que representaba la sociedad*".

También la SAN, Sala de lo Penal, nº 51/2014, de 3 de noviembre de 2014, Pte. Ilmo. Sr. D. Nicolás Poveda Peñas (JUR 2014\283335), que de conformidad con el artículo 369 *bis* condenaba por el delito contra la salud pública a la mercantil TRANSPINELO SL por su participación como instrumento jurídico respecto del delito contra la salud pública ordenando su disolución con perdida definitiva de su personalidad jurídica y su capacidad de realizar actividad comercial alguna, y al pago de multa; a la mercantil GEORMADRID MACHINERY SL por su participación como instrumento jurídico respecto del delito contra la salud pública ordenando su disolución con perdida definitiva de su personalidad jurídica y su capacidad de realizar actividad comercial alguna, y al pago de multa; y a la mercantil INVESTISSIMETN TRANS SPAIN AFRICA SA, por su participación como instrumento jurídico en respecto del citado delito contra la salud pública con la prohibición de realizar actividades comerciales en España por tiempo máximo de 5 años, y al pago de multa.

## CONCLUSIONES

***PRIMERA.-*** Las conductas de *hacking* constituyen una novedad vinculada a la revolución tecnológica acelerada que está experimentando nuestra sociedad en los últimos años. Estos comportamientos se ubican entre los supuestos conocidos como delincuencia informática. Fundamentalmente, los rasgos que los caracterizan son la aparición de una zona de riesgo con las nuevas tecnologías, común para muchos bienes jurídicos protegidos, la sencillez para su comisión, sin límites transfronterizos, despersonalización en la conducta, la vulnerabilidad de los equipos informáticos y la especilización en los sujetos que las realizan.

Precisamente, su naturaleza transnacional, así como los riesgos que estos nuevos mecanismos generan para los bienes jurídicos tradicionales y los que han surgido como consecuencia de estas nuevas formas de lesión, ha supuesto que las bases para su regulación y respuesta en el ámbito penal se hayan intentado sentar en el ámbito internacional, a través de diversos instrumentos de carácter vinculante en mayor o menor medida para los Estados miembros.

***SEGUNDA.-*** Las primeras regulaciones se establecen en torno al derecho a la *privacy*, que supera el tradicional derecho a la intimidad para referirse al problema de la acumulación de datos, ampliando poco a poco la inicial tutela civil y administrativa hacia el

amparo penal en Estados Unidos en los años 70 y en el ámbito de la Unión Europea en los años 80, comprendiendo en los años sucesivos las conductas de delincuencia económica y la piratería informática, considerando progresivamente que la comisión de cualquier delito puede verse favorecida por el uso de las nuevas tecnologías, hasta el punto de que surge un nuevo bien, la seguridad de los sistemas informáticos, que es digno de protección en los ordenamientos jurídicos. Considero que la revolución tecnológica acelerada conlleva la necesaria protección de este bien, que adquiere una progresiva mayor importancia a medida que se desarrollan las nuevas tecnologías.

***TERCERA.-*** Se han formulado distintos conceptos del fenómeno *hacking*, distinguiéndo el *hacker* blanco del *cracker*, que realiza el acceso para causar un daño al sistema o a su titular, *phreackers*, que utilizan los sistemas telefónicos para realizar interceptaciones sin ánimo de lucro, o los *viruckers*, cuya finalidad es introducir un virus en el sistema informático, de tal forma que el concepto gramatical identifica a los *hackers* como las personas que utilizan determinadas técnicas para el acceso si autorización a un sistema informático ajeno, habiendo optado la mayoría de los países por no distinguir la finalidad del *hacking*, poniendo fin a la distinción del *hacking* blanco y sancionar todos los supuestos de acceso a los sistemas ajenos.

Así pues, desde el punto de vista normativo se identifica *hacking* con *cracking*, razón por la cual se entiende que debe ser castigado. Es más, el legislador español opta por incluir como *hacking* también las conductas de mantenimiento no autorizado en un sistema informático ajeno, a pesar de que gramaticalmente no se podrían entender propiamente como supuestos de acceso ilícito.

***CUARTA.-*** En el ámbito español, la prevención de que la ley limitará el uso de la informática para garantizar el pleno ejercicio de los derechos se ubica en el artículo 18.4 de la Constitución de 1978, si bien la regulación específica del acceso no autorizado a los sistemas informáticos se inicia en 1980 con los grupos de estudio de la OCDE y la Convención del Consejo de Europa del año 1981. La respuesta en la legislación española a las corrientes internacionales se inicia en el ámbito civil y administrativo con la LO 5/1992, a la que sucedería la LOPD, creando la Agencia Española de Protección de datos.

La tipificación específica del *hacking* en España se produce por primera vez en el Código penal de 1995 con la reforma del año 2010. Hasta entonces los supuestos más graves eran reconducidos a los ataques contra la intimidad regulados en su artículo 197, sin perjuicio de que también pudieran considerarse un medio para cometer otros delitos. Entiendo que la reforma en nuestro Código penal era necesaria considerando el fácil acceso a Internet y a los distintos instrumentos que envuelven esta clase de delitos en nuestro

país, así como el momento en que nace el Convenio Europeo sobre Cibercriminalidad.

***QUINTA.-*** La reforma llevada a cabo por la LO 5/2010 en el Código penal supone la tipificación específica del *hacking*, que trae consecuencia de la DM 2005/222/JAI.

Los trámites parlamentarios de la referida reforma se inician en el año 2006, considerando la necesidad de responder a las nuevas modalidades delictivas y armonizar la legislación española con la europea. Aunque esa normativa se refiere tanto al acceso no autorizado a sistemas informáticos como a su perturbación y a los daños a los datos y sistemas informáticos, el legislador opta por tipificar separadamente esos daños y el acceso. Además, desde el Anteproyecto de Reforma de 2009 el legislador español incluye los supuestos de mantenimiento no autorizado en el sistema informático en el artículo 197 del Código penal, conducta que no estaba prevista en la DM 2005/222/JAI.

Durante los trámites parlamentarios fueron especialmente objeto de debate la responsabilidad de las personas jurídicas y la inclusión del apartado 8 del artículo 197, relativo a la comisión en el seno de organización o grupo criminal. Las propuestas de supresión fueron rechazadas.

***SEXTA.-*** El artículo 197.3, relativo al acceso ilícito a los sistemas informáticos fue reformado por la LO 1/2015, como consecuencia de la Directiva 2013/40/UE, que traslada esas conductas al artículo 197 *bis* 1, incluyendo como novedad el castigo en el mismo precepto de las conductas de facilitar a otro el acceso y la referencia al hecho del acceso al sistema de información. Esto supone la sustitución de la anterior mención a datos o programas informáticos. Además, se incluye en el artículo 197 *ter* la conducta de facilitar la comisión del delito, que puede plantear problemas interpretativos con el tipo básico; en el artículo 197 *quater* se habla de la comisión del delito por organizaciones o grupos criminales; y en el artículo 197 *quinquies* se incluye la responsabilidad de la persona jurídica. La introducción de estos preceptos a través de cinco enmiendas tiene la peculiaridad de que no viene precedida de los dictámenes previos del Consejo Fiscal, CGPJ y Consejo de Estado. La explicación se debe a que la Directiva 2013/40/UE fue publicada en el DOUE de 14 de agosto de 2013 y los nuevos artículos fueron consecuencia de las enmiendas del Grupo Popular aceptadas en el Congreso de los Diputados, que fueron posteriores a los citados dictámenes elaborados sobre el texto que en principio se iba a reformar.

***SÉPTIMA.-*** La regulación de las conductas de *hacking* en la mayoría de los países de nuestro entorno europeo no es lo suficientemente minuciosa, limitándose a la regulación del tipo básico y omitiendo otros supuestos que pueden surgir en torno al intrusismo

informático. Tampoco dotan a estas conductas de la debida autonomía respecto de otras, originando problemas interpretativos similares a los que acontecen en el Código Penal español.

Así, aunque algunos países incluyen una amplia regulación del acceso a los sistemas informáticos y sus variantes (Croacia, Finlandia, Hungría, Malta, Portugal y Reino Unido), la mayoría de legislaciones europeas regulan esas conductas en las mismas o distintas ubicaciones sistemáticas. Entre los delitos contra la intimidad (Alemania, Austria, Grecia y Polonia), entre los delitos contra el honor y otros derechos individuales (Dinamarca), contra la propiedad (Eslovaquia, Eslovenia, Estonia, Francia, Malta, República Checa y Luxemburgo), contra el orden público (Holanda), junto a otros delitos de daños (Irlanda), contra la inviolabilidad del domicilio (Italia), contra la libertad y la paz (Suecia), o contra la seguridad (Letonia, Lituania y Rumanía). Esta variedad genera confusión en la delimitación del bien jurídico protegido.

Son minoría los países que tipifican sistemáticamente las conductas entre los delitos informáticos (Chipre, Irlanda, Portugal y Reino Unido) o, al menos, les otorgan cierta autonomía en un título o capítulo propio y diferenciado (Bélgica, Bulgaria, Croacia, Finlandia o Hungría).

En consecuencia, son muy pocos los países que tipifican detalladamente el *hacking*, es decir, realizan una amplia regulación del delito y sus variantes, y, además, lo hacen de forma sistemática y separada de otros delitos que no están relacionados con estas

conductas. En concreto, los citados Croacia, Finlandia, Hungría, Portugal y Reino Unido. De entre ellos, además, en el caso de Hungría y Portugal su tipificación es anterior incluso a ratificar el Convenio Europeo sobre Cibercriminalidad en el año 2003.

***OCTAVA.-*** Considero que es un acierto optar por una regulación unitaria de los delitos informáticos, atendida la evolución acelerada en la materia y la amplitud de bienes jurídicos que pueden verse afectados a través de la informática. Si se optara por un modelo similar, tipificando estas conductas en una norma, título o capítulo autónomo, delimitando claramente su bien jurídico protegido, estableciendo definiciones sobre los conceptos básicos y regulando a continuación el tipo básico y sus modalidades, sin duda ayudaría al intérprete en un campo tan complejo y en continuo cambio como el que nos ocupa en este trabajo, y podría evitar la amalgama de articulos, remisiones y referencias que actualmente se encuentra en el Código Penal español sobre esta materia.

***NOVENA.-*** La regulación del *hacking* en los países de nuestro entorno europeo que han optado por un orden sistemático muestra que no era inevitable introducir el artículo 197.3 en el ordenamiento interno español con la LO 5/2010 entre los delitos contra la intimidad, para luego intentar solventar el caos sistemático con la reforma de la

LO 1/2015, originando mayor confusión, sino que era posible una regulación ordenada de estos nuevos delitos.

***DÉCIMA.-*** En definitiva, la reforma llevada a cabo por la LO 1/2015 adolece de cierta rotundidad. Se ha desaprovechado la oportunidad de separar claramente los delitos contra la intimidad y el *hacking*, incluso para establecer una regulación unitaria de los delitos informáticos, en la medida en que se ha optado por dejar el contenido del anterior artículo 197.3 en el siguiente artículo, el 197 *bis* 1, dentro del mismo Capítulo. No obstante, esa nueva regulación puede ser un primer paso para una futura agrupación de estos delitos en un apartado propio del Código Penal, de tal forma que se consiga un tratamiento sistemático del precepto acorde con el bien jurídico protegido, facilitando su interpretación tal y como ha sucedido en otros países de nuestro entorno como Bélgica, Bulgaria, Croacia, Finlandia o Hungría.

***UNDÉCIMA.-*** Según se viene exponiendo, el artículo 197 *bis* 1 presenta dificultades interpretativas por su ubicación sistemática. Por la descripción típica parece que se trata de proteger la seguridad de los sistemas, como presupuesto para que la informática pueda desempeñar su función social, siendo necesaria su tutela y adelantando así la barrera de protección de otros bienes jurídicos. Por ello, no resulta adecuada su ubicación en el Título X del CP, entre los delitos

contra la intimidad, que parece indicar que éste sería el bien jurídico protegido.

***DUODÉCIMA.-*** Atendiendo a los compromisos internacionales por los cuales se introdujo el artículo 197.3 del CP por la LO 5/2010 y después el 197 *bis* 1 del CP por la LO 1/2015, la seguridad de los sistemas informáticos (abarcando la confidencialidad, la integridad y la disponibilidad de los sistemas informáticos) resulta ser el bien jurídico directamente protegido por este precepto, considerando además la menor pena que conllevan estas conductas en relación con las previstas en los apartados 1 y 2 del artículo 197 CP. Estos son los intereses recogidos en el Preámbulo del Convenio Europeo sobre Cibercriminalidad, en los considerandos 1 y 2 de la DM 2005/222/JAI y en el Considerando 26 de la Directiva 2013/40/UE.

***DECIMOTERCERA.-*** La legislación europea no excluye la protección de la intimidad con este nuevo delito, que es lo que parece pretender el legislador español al incluir el tipo entre los delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio, si bien en este caso considero que podemos hablar de un bien jurídico protegido de una forma indirecta. Ahora bien, entiendo que la tutela indirecta no se limita a ésta, sino también a otros bienes jurídicos, en la medida que la regulación del *hacking* supone adelantar

las barreras de protección de los bienes jurídicos que con el acceso y la puesta en peligro del sistema puedan verse afectados, como podrían ser también, el patrimonio, la propiedad o los secretos de empresa

***DECIMOCUARTA.-*** Por otra parte, el conjunto o parte del sistema de información se presenta como el objeto material del delito de *hacking* en nuestro Código. El hecho de que con la LO 1/2015 se pase de la referencia a los datos o programas informáticos al conjunto o una parte del sistema evidencia el adelantamiento de la protección para los bienes jurídicos individuales que pudieran verse afectados por el acceso y, a su vez, un distanciamiento de la intimidad como bien jurídico protegido.

***DECIMOQUINTA.-*** La nueva terminología resulta más acertada que la limitada por el acceso a datos o programas informáticos para la tutela del bien jurídico protegido, por cuanto permite incluir supuestos que son igualmente atentatorios contra la seguridad del sistema, como puedan ser los programas espía que se instalan una vez se ha accedido al mismo. Aunque el legislador no ha introducido en el Código un concepto para sistema de información, cabe entender como tal el referido al sistema informático, si se atiende a las definiciones que ofrecen los instrumentos internacionales que inspiran la reforma realizada por la LO 1/2015. Además, la referencia expresa al citado objeto material, abandonando los datos o programas

informáticos, deja a un lado el problema de delimitación con las conductas del artículo 197.2 CP, relativo al acceso a datos de carácter personal o familiar registrados en ficheros o soportes informáticos.

***DECIMOSEXTA.-*** Entiendo que la protección de los sistemas de información, comprendiendo la confidencialidad, integridad y disponibilidad, sin exigir su efectivo menoscabo, determina que es un delito de peligro concreto para la seguridad del sistema informático afectado.

***DECIMOSÉPTIMA.-*** Si con el acceso o el mantenimiento en el sistema también se produjera un riesgo o lesión para otros bienes jurídicos, tendría lugar una relación concursal. De igual forma, si resultase la destrucción o menoscabo de la confidencialidad, integridad o disponibilidad del sistema, estaríamos ante un concurso entre el *hacking* por haber causado el peligro concreto a ese bien jurídico y el delito de daños o contra la intimidad que se hubiese producido.

***DECIMOCTAVA.-*** Considero que no es suficiente con el mero acceso vulnerando medidas de seguirdad o el mantenimiento no autorizado a un sistema informático, sino que se debe ver afectada la seguridad del sistema. Debe existir un resultado de peligro efectivo sobre la confidencialidad, integridad o disponiblidad del sistema, bien

al que por otra parte se refiere la normativa comunitaria que fundamenta la introducción del tipo en el Código Penal, razón por la cual entiendo que se trata de un delito de resultado de peligro concreto en ambos supuestos, evitando la excesiva amplitud del delito que conllevaría castigar cualquiera de esas conductas aunque no hubiese existido un peligro para la confidencialidad, integridad o disponibilidad del sistema al que se accede o en el que se permanece, con la posible contradicción con los principios de intervención mínima, legalidad y ofensividad.

***DECIMONOVENA.-*** En el nuevo artículo 197 *bis* 1 el acceso no autorizado a todo o parte de un sistema de información y la vulneración de las medidas de seguridad establecidas para impedirlo son los elementos que definen las conductas de *hacking*.

El legislador no se ha detenido en que el sujeto tenga capacidad potencial para acceder a cualquier tipo de información que se encuentre en el sistema, alejándose de la definición de *hacking* mantenida por parte de la doctrina con ocasión del anterior artículo 197.3.

***VIGÉSIMA.-*** Atendiendo al tenor literal del vigente artículo 197 *bis* 1 y considerando el principio de legalidad, en nuestro Derecho penal el *hacking* es el equivalente al intrusismo informático o violación de una esfera de exclusividad del titular del sistema, siendo

intrascendente el contenido del sistema, y resultando suficiente el mero acceso no autorizado al sistema de información o parte del mismo vulnerando las medidas de seguridad establecidas para impedirlo, si se ha puesto en peligro su confidencialidad, integridad o disponibilidad, con independencia de que se acceda o no a los datos.

***VIGÉSIMA PRIMERA.-*** Se ha criticado la equiparación en el mismo párrafo de las conductas de mantenimiento en el sistema informático con las de acceso ilícito, porque éste puede conllevar un acceso a datos y programas tal y como se regulaba en el anterior artículo 197.3, mientras que la permanencia en el sistema previo acceso lícito sólo supone un peligro para los datos o programas que puedan haber en el sistema informático en cuanto puedan ser conocidos o utilizados y por tanto tan sólo implicaría un peligro indirecto para la confidencialidad e integridad del sistema informático. Sin embargo, entiendo que, aunque habría sido deseable una mayor concreción de los supuestos de mantenimiento o su regulación de forma autónoma a efectos de no equipararlas con el *hacking* en sentido propio, pueden ser igualmente peligrosos para la confidencialidad, integridad o disponibilidad del sistema informático, no estando referido actualmente el delito de *hacking* a los citados datos o programas.

***VIGÉSIMA SEGUNDA.-*** El delito de *hacking* requiere el

acceso al conjunto o una parte de un sistema de información con su puesta en peligro, por lo que, será posible que el sujeto no consiga saltarse las medidas pese a su intención de hacerlo y haber iniciado la acción, produciéndose la tentativa inacabada, o que habiendo sido capaz de saltarlas, no pueda acceder al sistema, dando lugar a la tentativa acabada; y además, es un delito de medios indeterminados, comprendiendo cualquier tipo de conductas que determinen el acceso. Se equiparan a estos supuestos los relativos a facilitar ese acceso, dentro del mismo artículo 197 *bis* 1, o incluso facilitar el mantenimiento en el sistema por los medios o instrumentos que cita en el artículo 197 *ter*, por lo que parece evidente que el legislador ha intentado comprender todos los casos, tanto de efectivo acceso como de facilitarlo, en la protección de la seguridad de los sistemas informáticos.

***VIGÉSIMA TERCERA.-*** La tipificación del acceso a todo o parte de un sistema de información resulta más acertada para la efectiva protección de su seguridad que la limitada por el acceso a datos o programas informáticos, dando cabida así a supuestos que son igualmente atentatorios contra el bien jurídico protegido, como el caso de la instalación de un programa espía tras el acceso al sistema. Además, la mención a ese objeto material, abandonando los datos o programas informáticos, evita el problema de delimitación con las conductas del artículo 197.2 CP.

***VIGÉSIMA CUARTA.-*** La tipificación de las conductas de "facilitar el acceso", equiparándolas en el mismo precepto con el "acceso", supone igualar los casos de autoría y participación. Por ello parece razonable entender que en estos comportamientos es necesario que se llegue a producir el "acceso". Así se evitaría el contrasentido de castigar al que facilita la conducta de acceso como si hubiese llevado a cabo, siendo que no se ha producido. De esta forma también se delimitarían estos supuestos con los del artículo 197 *ter*, donde no sería necesario el cumplimiento de esa conducta de acceder.

***VIGÉSIMA QUINTA.-*** Entiendo posible que las conductas se realicen por cualquier medio, incluso por omisión al no estar excluida, agotándose el tipo subjetivo con el dolo en cuanto conocimiento y voluntad de acceder o permanecer en el sistema, o facilitar el acceso, sin autorización y quebrantando las medidas de seguridad establecidas para impedirlo.

***VIGÉSIMA SEXTA.-*** El mero acceso al sistema informático no necesita la afección continuada a su seguridad, es decir, es un delito instantáneo por cuanto, producido ese acceso con la puesta en peligro para el sistema, la conducta habría finalizado y no permanecería en el tiempo. Sin embargo, en las conductas de mantenimiento no autorizado en el sistema, el verbo típico y la flexibilidad del bien jurídico determinan en este caso la naturaleza

permanente del delito, al existir la persistencia que caracteriza este tipo de delitos mientras el sujeto se mantenga en el sistema sin autorización.

***VIGÉSIMA SÉPTIMA.-*** El elemento de las medidas de seguidad resulta de tal importancia en la tipicidad de la conducta que sin medidas no hay ilícito penal y, a su vez, evidencian la voluntad del titular de no autorizar el libre acceso.

Como medidas de seguridad se pueden considerar todas las aplicaciones o herramientas, incluso de naturaleza física y no sólo informáticas, establecidas específicamente para impedir el acceso, por cuanto ponen de manifiesto que el titular ha constituido medios para impedir el libre acceso a su domicilio informático, tratando de evitar intrusiones no autorizadas y salvaguardando así la seguridad del sistema. Parece lógico entender el concepto de una forma restrictiva, es decir, que sean medidas fijadas con la finalidad específica de impedir el *hacking*. Esto llevará a una labor interpretativa en cada caso, excluyendo las que no vengan referidas de forma individualizada al acceso, evidenciándose el empleo de un elemento normativo social o cultural por el legislador.

***VIGÉSIMA OCTAVA.-*** El consentimiento tiene que ser debido tras la reforma de la LO 1/2015 y, por tanto, indubitado, sea expreso o tácito, conforme a la jurisprudencia y a la doctrina

constitucional.

***VIGÉSIMA NOVENA.-*** El Código no especifica la capacidad de la persona que puede otorgar la autorización y esto obliga a considerar las condiciones concurrentes en cada caso, descartando el consentimiento del absolutamente incapaz, considerando los riesgos que contiene ese consentimiento y la comprensión por parte de quien lo otorga.

***TRIGÉSIMA.-*** La autorización puede provenir del propietario del sistema o el titular legítimo, y esa autorización delimitará el acceso consentido, pudiendo ponerle fin en cualquier momento. La autorización judicial está prevista en la normativa procesal.

El consentimiento obtenido a través de la solicitud de autorización para el acceso, supone la atipicidad de las denominadas *cookies*. De igual forma, será el usuario quien también va a delimitar hasta dónde acceden estos bloques de datos que se almacenan en su sistema.

***TRIGÉSIMA PRIMERA.-*** Tanto el artículo 197 *bis* 1 como el artículo 197 *ter* CP se refieren a facilitar la comisión del delito, por lo que puede producirse confusión entre ambos supuestos.

En principio, entiendo que el artículo 197 *ter* se refiere a

proporcionar instrumentos concretos para el acceso, pero la referencia en el mismo precepto a facilitar "*datos similares*" a "*una contraseña de ordenador*" o "*un código de acceso*" de nuevo puede plantear problemas de confusión. En estos casos se produciría un concurso de normas que en principio se resolverá conforme al principio de especialidad del artículo 8 CP a favor del 197 *ter*, pero en la práctica será difícil esa solución, atendida la redacción del artículo 197 *ter*, con alusiones a "*de cualquier otro modo, facilite a terceros*". Atendida esa extensión del artículo 197 *ter*, al artículo 197 *bis* le quedaría un carácter residual, donde tendrán cabida las restantes conductas de facilitar el acceso ilícito atendida la falta de concreción de los medios en este caso y que en la práctica llevaría a pensar en principio tan sólo en aquellos supuestos en los que se suministren instrumentos de naturaleza no informática para la comisión del delito.

Pero incluso con esa solución, esa referencia del artículo 197 *ter* a las conductas de quien "*de cualquier modo, facilite a terceros*" alguno de los citados medios, incluso deja poco margen para interpretar esos hipotéticos supuestos del 197 *bis* 1. Por ello, considero en estos casos como elemento diferenciador la circunstancia de que en el caso del artículo 197 *bis* 1 se requiere que se produzca el efectivo acceso al sistema por el sujeto al que se le ha facilitado, lo cual no es necesario en el supuesto del 197 *ter* al tratarse de un acto preparatorio.

***TRIGÉSIMA SEGUNDA.-*** Con el nuevo adelantamiento de la barrera de protección de los bienes jurídicos al momento de facilitar

las conductas del acceso, no parece que fuese necesario incluir el artículo 197 *ter* atendida la existencia del 197 *bis* 1 CP, resultando inadecuado por los problemas interpretativos que plantea.

***TRIGÉSIMA TERCERA.-*** En las conductas de mantenimiento en el sistema informático tiene que existir una autorización previa al acceso y la pérdida expresa o tácita de ésta. Si no existiese una autorización previa, nos encontraríamos ante las conductas de acceso ilícito y, por otra parte, en el caso de que no se hubiera perdido la autorización inicial, existiría un mantenimiento lícito dentro del sistema.

***TRIGÉSIMA CUARTA.-*** Atendida la redacción del artículo 197 *bis* 1, uno de los problemas en la interpretación del artículo se encontrará en la exigencia o no de vulneración de medidas de seguridad en la permanencia en el sistema, por cuanto el legislador no ha sido claro. Entiendo que el elemento determinante es mantenerse en él "*contra la voluntad de quien tenga el legítimo derecho a excluirlo*" y no el de la vulneración de medidas de seguridad. Se trata por tanto de supuestos de entrada inicialmente permitida cuya autorización es retirada posteriormente, siendo indiferente que existan o no medidas de seguridad. Mientras se exige que el acceso se lleve a cabo con vulneración de esas medidas, las medidas no se habrán vulnerado por quien entra en el sistema con autorización, supuesto

distinto a que una vez en el sistema, denegado el mantenimiento se modifiquen las medidas y se quebranten, en cuyo caso nos encontraríamos de nuevo en la primera de las conductas de acceso ilícito.

***TRIGÉSIMA QUINTA.-*** Se pone en evidencia de nuevo la defectuosa técnica legislativa al incluirse las conductas de facilitar el mantenimiento en el sistema por alguno de los medios que cita en el artículo 197 *ter* y, sin motivo alguno, no se incluyan igualmente dentro del artículo 197 *bis* 1, tal y como sucede con los supuestos de acceso.

***TRIGÉSIMA SEXTA.-*** En el supuesto de *hacking*, la falta de autorización es lo que atribuye relevancia penal a la conducta, configurándose como un delito doloso. Dolo que se refiere a la consciencia y voluntad de acceder sin autorización al sistema de información, vulnerando las medidas de seguridad, o mantenerse dentro del sistema en contra de la voluntad de quien tenga el legítimo derecho a excluirlo, o bien, tras la reforma de la LO 1/2015, con conocimiento y voluntad de facilitarlo.

En cuanto al error sobre esos elementos, la exigencia de que se vulneren medidas de seguridad hará difícil en la práctica apreciar un supuesto en el que el sujeto quebrante esas medias y no se aperciba de ello. Será más fácil pensar en el error de tipo en un sujeto que creyese

que está facilitando a otro sujeto el acceso al que se considera su sistema informático, siendo que en realidad se está accediendo ilícitamente a un sistema ajeno.

Cuestión distinta será que el error recaiga sobre la ilicitud del acceso al sistema informático ajeno, en cuyo caso parece razonable considerar el error de prohibición con las consecuencias del artículo 14.3 CP. En este caso resulta complicado en la práctica que pueda darse el error de prohibición en el *hacking*.

Son posibles los supuestos de dolo eventual, tal y sucedería en el caso del sujeto que pretende superar la medida de seguridad de un sistema informático como reto personal, asumiendo como posible que con el quebrantamiento de esa medida se producirá el acceso al mismo.

***TRIGÉSIMA SÉPTIMA.-*** En cuanto a las figuras de la autoría y la participación en el delito de *hacking*, se parte de la teoría del dominio del hecho.

De esta forma, para que exista coautoría en el delito de *hacking* será preciso que el acceso se produzca de forma concertada entre varios sujetos, interviniendo cada uno de ellos en su ejecución como autores, todos ellos con dominio del hecho consistente en el acceso ilícito o en el mantenimiento en el sistema.

También resultaría posible la autoría mediata en estos delitos, como sucedería en el caso de que el dominio del hecho se llevase a

cabo mediante coacción, por violencia o amenazas sobre un sujeto para que realice el acceso ilícito al sistema informático o el mantenimiento no autorizado en el sistema.

***TRIGÉSIMA OCTAVA.-*** Es posible la inducción en supuestos tales como el del sujeto que influye en otro para que lleve a cabo el acceso ilícito o el mantenimiento en un sistema de información, siempre y cuando el sujeto que lo ejecuta no estuviese ya decidido a cometer el delito antes, y siendo necesaria la efectiva ejecución.

***TRIGÉSIMA NOVENA.-*** Puesto que no existe una tipificación expresa, no existiría castigo para la proposición, provocación y conspiración para delinquir en estos casos, salvo si un sujeto incitase directamente *"por medio de la imprenta, la radiodifusión o cualquier otro medio de eficacia semejante, que facilite la publicidad, o ante una concurrencia de personas, a la perpetración de un delito"* de *hacking*, porque "*Si a la provocación hubiese seguido la perpetración del delito, se castigará como inducción"* (artículo 18.2 CP).

***CUADRAGÉSIMA.-*** La distinción práctica entre la autoría y la cooperación necesaria en el delito de *hacking* ha quedado difuminada en la medida en que tras la LO 1/2015 serán autores tanto el que "*acceda*" como el que "*facilite a otro el acceso*".

También resulta difícil pensar en algún supuesto de complicidad en el delito del artículo 197 *bis* 1 CP, tras la equiparación de las conductas entre el que "*acceda*" y el que "*facilite a otro el acceso*", produciéndose una criticable ampliación de los supuestos de autoría a los supuestos que tendrían la consideración de participación.

La complicidad se reduciría a las conductas de facilitar el acceso que no estén previstas en los artículos 197 *bis* 1 o 197 *ter*, limitándose a los casos en los que el sujeto ayuda al acceso al sistema informático siempre que no lo hiciera facilitando los instrumentos del artículo 197 *ter* CP y, además, el acceso no tuviese éxito, eludiendo de esta forma la autoría del artículo 197 *bis* 1 CP. En el caso de las conductas de mantenimiento no autorizado en el sistema, se deberían relizar actos accesorios o periféricos, con conocimiento del propósito criminal del autor y voluntad de contribuir a esa permanencia por algún medio no encuadrable en el artículo 197 *ter* CP.

***CUADRAGÉSIMA PRIMERA.-*** En la fase externa del delito de *hacking* se sigue la doctrina de los actos unívocos por resultar la más sencilla a efectos de delimitar los actos preparatorios del *hacking*. De esta forma, cuando el sujeto realice actos que por sí mismos evidencien unívocamente la intención de acceder o mantenerse ilícitamente en el sistema o facilitar el acceso, estaremos en la fase de ejecución del delito tipificado en el artículo 197 *bis* 1 CP, mientras que cuando el acto que se realice pueda llevar a la ejecución del delito o a cualquier otro acto no ofensivo, será un acto preparatorio impune.

Se tipifican expresamente los actos preparatorios de estos delitos en los artículos 197 *bis* 1 y 197 *ter* CP, produciéndose un *iter criminis* expansivo, en el que se anticipa la tutela de la seguridad de los sistemas informáticos incluso al momento de facilitar la conducta.

***CUADRAGÉSIMA SEGUNDA.-*** Las resoluciones manifestadas, consistentes en la provocación, conspiración y proposición, no están castigadas en el caso del intrusismo informático del artículo 197 *bis* 1 CP, sin perjuicio del castigo al inductor en la forma ya mencionada.

***CUADRAGÉSIMA TERCERA.-*** En la tentativa se distingue la acabada e inacabada por una parte, y el desistimiento y el arrepentimiento activo por otra. Así, será posible que el acceso no se produzca, porque una vez iniciado el proceso el sujeto no sea capaz de quebrantar las medidas de seguridad (tentativa inacabada) o porque vulneradas no se consiga acceder al sistema de información (tentativa acabada). Así, si considerado los actos, instrumentos y la mecánica empleada por el sujeto para llevar a cabo el acceso, se hubiese podido producir objetivamente el resultado del acceso al sistema pretendido, estaremos ante la tentativa acabada del delito del artículo 197 *bis* 1 CP, mientras que si no se hubiese podido alcanzar el resultado, será la modalidad inacabada.

***CUADRAGÉSIMA CUARTA.-*** Se producirá el desistimiento si el sujeto que inicia el delito de *hacking*, de forma voluntaria, personal y definitiva, y sin ningún obstáculo insuperable que le impidiese acceder al sistema, decide no culminar todos los actos de ejecución. Por el contrario, si ha surgido un obstáculo insuperable para alcanzar ese resultado, impidiendo la ejecución de todos los actos, no existirá un desistimiento, sino una tentativa inacabada. El sujeto no accederá porque no puede acceder.

***CUADRAGÉSIMA QUINTA.-*** Si se han ejecutado todos los actos para el acceso, y el resultado no se produce por la decisión del sujeto que realiza ese acceso, tendrá lugar el arrepentimiento activo. Sin embargo, si no ha sido el sujeto quien ha llevado la actuación para evitar que el acceso se produzca, entiendo que se producirá la tentativa acabada.

***CUADRAGÉSIMO SEXTA.-*** Sería posible la tentativa inidónea, como sucedería si se pretendiera acceder desde un *e-reader* al sistema del CNI, y el delito imposible, como en el caso del sujeto que entra en un edificio para llegar hasta el habitáculo donde supuestamente se encuentra su sistema informático y allí acceder al mismo, pero una vez en el lugar comprueba que el edificio no cuenta con sistema informático.

***CUADRAGÉSIMA SÉPTIMA.-*** Por las características de las conductas de permanencia en el sistema por una parte, donde la consumación se determina en cada caso atendiendo al momento hasta donde el sujeto estaba autorizado y la capacidad para poner en peligro concreto el sistema, y las de facilitar el acceso por otra parte, donde si no se alcanza el acceso la conducta se encuadrará en el artículo 197 *ter*, desde mi punto de vista será difícil que en la práctica pueda darse la tentativa en alguno de estos supuestos.

***CUADRAGÉSIMA OCTAVA.-*** En las relaciones concursales entre las conductas de *hacking* y otros delitos, se plantea el concurso de facilitar el acceso con la de facilitar la conducta, prevista en el artículo 197 *ter*, donde habrá que considerar si efectivamente se produce el acceso. En este caso, por coherencia penológica entre acceder y facilitar sería encuadrable la conducta en el artículo 197 *bis* 1, mientras que si no se llega a producir el acceso, dada la especialidad de los medios en el artículo 197 *ter*, se debería resolver el concurso a favor de la aplicación de este último precepto.

En el caso en el que el sujeto facilita medios para la comisión del *hacking* y a su vez también lleva a cabo el delito del artículo 197 *bis* 1 entiendo más adecuado considerar la conducta como un delito continuado de acceso ilícito.

***CUADRAGÉSIMA NOVENA.-*** En el concurso con el allanamiento de morada, si fuese necesario un acceso físico al espacio (morada) donde se encuentra el sistema informático, como infracción más grave, el acceso ilícito al sistema informático absorberá ese delito con las consecuencias del artículo 77.3 CP.

***QUINCUAGÉSIMA.-*** Cuando el sujeto accediese al sistema informático apoderándose de datos reservados o sin estar autorizado acceda a ellos dará dar lugar al concurso de normas entre el delito del artículo 197 *bis* 1 CP y el del artículo 197.2 CP, quedando absorbido por éste último. Así, ante la identidad de bienes jurídicos o al menos de línea de ataque, se aplicaría el criterio de la consunción del delito cuyo umbral típico se ubica más lejos de la afección al bien jurídico protegido.

***QUINCUAGÉSIMA PRIMERA.-*** Cabe la posibilidad que el instrusismo sea paso previo para la comisión del delito de daños informáticos regulado en el artículo 264 CP. En este caso, la tentativa del delito de daños cuando no se llega a causar el daño por causas independientes a la voluntad del autor, constituiría un delito consumado de *hacking*, al configurarse como un delito autónomo de peligro concreto que conllevaría mayores penas que la tentativa de daños, a la que absorbería.

En el caso de que el daño pretendido sea efectivamente causado una vez producido el acceso, se produciría un concurso ideal en su versión medial, en cuanto el acceso se configura como un medio necesario para causar el daño, que absorbería al *hacking*.

Ahora bien, si consumado el intrusismo, se decidiera causar daños informáticos o, al revés, cuando provocados daños informáticos, se realizase el acceso ilícito con posterioridad, tendría lugar un concurso real.

***QUINCUAGÉSIMA SEGUNDA.-*** Si el acceso ilícito a un sistema de información se configura como paso previo a la comisión de otros delitos, pueden producirse numerosas situaciones concursales. Así, los casos del delito de *grooming* (artículo 183 *ter*), donde se produciría un concurso real de delitos, por cuanto no podría considerarse el acceso al sistema informático como un medio que fuera únicamente dirigido al contacto con el menor, sino que al menos causaría también un peligro de la intimidad y datos personales del menor. A la misma conclusión se llegaría si el acceso al sistema informático ajeno fuese para la captación de menores con finalidad exhibicionista o pornográfica, prevista en el artículo 189 CP.

***QUINCUAGÉSIMA TERCERA.-*** Si el acceso ilícito fuese para la comisión de un delito de estafa informática (artículo 248.2 CP), en este caso, la nueva configuración del delito referido al mero

acceso al sistema, como delito de peligro y de resultado, donde existe un nuevo bien jurídico como es la seguridad de los sistemas informáticos, daría lugar a un concurso de normas donde siendo en el *hacking* el bien jurídico tan sólo la seguridad informática de forma directa, se encontraría en un peldaño inferior respecto a otros delitos para cuya comisión se haya tenido que pasar por vulnerar un sistema informático, hablando así de la progresión delictiva, es decir, concurso de normas que considero deberá solventarse conforme al principio de especialidad o alternatividad a favor del delito de estafa.

***QUINCUAGÉSIMA CUARTA.-*** En el mismo sentido, también existiría un concurso de normas en los delitos de defraudaciones de fluido eléctrico y análogas (artículos 255 y 256 CP), en los casos en que se accediese al sistema informático ajeno para cometer una defraudación utilizando energía o para hacer uso de un equipo terminal de comunicación. Igualmente, cuando el acceso se produce para cometer un delito contra la propiedad intelectual del artículo 270 CP, especialmente cuando se accede para realizar copias ilegales de programas informático o se facilita el acceso ilegal en Internet. Y el citado argumento también resultaría válido para otras conductas como las injurias o calumnias con publicidad (artículo 211 CP), el descubrimiento de secretos de empresa (artículo 278.1 CP), incitación al odio, hostilidad, discriminación o violencia (artículo 510.1.a CP), daños a líneas de telecomunicaciones (artículo 560.1 CP), enaltecimiento del terrorismo (artículo 578.1 CP) o

descubrimiento de secretos relativos a la defensa nacional (artículo 598 CP).

***QUINCUAGÉSIMA QUINTA.-*** La agravante del artículo 197 *quater* está prevista para los supuestos en que las conductas se cometan en el seno de organizaciones o grupos criminales, aplicándose las penas superiores en grado a todas las conductas del capítulo. En el anterior artículo 197.8 la referencia era únicamente a las conductas del artículo 197, lo que llevaba una agravación desproporcionada. Tras la LO 1/2015 el *hacking* tiene su regulación específica en el artículo 197 *bis* 1, por lo que ya no tiene lugar la aplicación de la agravante de llevar a cabo la conducta en el seno de una organización o grupo criminal sobre, por ejemplo, el *hacking* con ánimo de lucro que estaba prevista en el anterior artículo 197.7, por lo que el legislador ha moderado la agravante.

En cuanto al fundamento, se trata de una agravante mixta, donde concurren elementos objetivos y subjetivos, y con la que se pretende prevenir y mejorar la lucha contra la criminalidad organizada a través de las nuevas tecnologías, atendido el incremento en el desvalor de la acción y del resultado, lo que fundamenta el mayor castigo.

***QUINCUAGÉSIMA SEXTA.-*** El sujeto que accede desde su domicilio a Internet, a una comunidad que tiene un claro objeto

delictivo, como sería una comunidad de *hackers*, donde el objeto es acceder a otros sistemas informáticos ilícitamente o compartir y recibir información o medios para hacer posible el acceso, lo hace participando de una organización criminal porque concurren más de dos personas, en una comunidad o *web*, sabiendo que accede a un sitio donde es sencilla la comisión del delito. Todo ello, salvo que se tratara de un mero acceso del sujeto a la comunidad de forma accidental u ocasional, por cuanto es necesario pluralidad de personas coordinadas entre sí y una mínima permanencia para superar la mera codelincuencia.

***QUINCUAGÉSIMA SÉPTIMA.-*** Por último, no se entiende la equiparación de penas en el artículo 197 *quater* cuando el delito es cometido en el seno de una organización o de un grupo criminal, atendida la distinción conceptual y penológica en los artículos 570 *bis* y 570 *ter* y el fundamento que el propio legislador establece en el Preámbulo de la LO 5/2010 para las mayores penas en el caso de organizaciones criminales. Considero que de forma coherente se debería haber eliminado el artículo 197 *quater*, llevando estas conductas a los artículos 570 *bis* y 570 *ter*, o bien se debería haber mantenido el artículo 197 *quater* con una diferenciación de penas en función de que la conducta se lleve a cabo en el seno de una organización o grupo criminal, atendida la clara distinción legal y jurisprudencial entre los dos niveles de riesgo par los bienes jurídicos

protegidos según se trate por una parte de organización o, por otra, de grupo criminal.

***QUINCUAGÉSIMA OCTAVA.-*** La taxatividad del tipo del artículo 198 CP impuesta por el principio de legalidad conlleva su inaplicación práctica al supuesto del artículo 197 *bis* 1 CP, por cuanto tras la reforma de la LO 1/2015, el anterior artículo 197 pasa a dividirse en varios artículos, mientras el artículo 198 CP sigue manteniendo la misma redacción, es decir, sólo se aplica a la autoridad o funcionario público que "*realizare cualquiera de las conductas descritas en el artículo anterior*", lo que significa su única aplicación a los supuestos del artículo 197 *quinquies*, relativo a la responsabilidad de la persona jurídica. Esta situación supone establecer una barrera para los órganos jurisdiccionales que tienen que aplicarlo, en la medida que cuando se les presente el caso de una autoridad o funcionario público que cometa el delito que estamos estudiando, no podrán realizar una interpretación extensiva y analógica del precepto, conforme ordena el artículo 4.1 CP.

No obstante, la agravante se ha analizado en este trabajo desde el punto de vista de su aplicación futura a los supuestos de intrusismo informático.

***QUINCUAGÉSIMA NOVENA.-*** El artículo 198 guarda similitud con los artículos 414, 415 ó 536 CP.

En el caso del artículo 414 CP se exige que se trate del acceso a documentos y no meramente a un sistema informático que pueda contenerlos. Por su especialidad y mayor gravedad determina que se deberá resolver a su favor un hipotético concurso de normas con las conductas de facilitar el acceso a un sistema del artículo 197 *bis* 1 CP.

***SEXAGÉSIMA.-*** En relación con el artículo 415 CP, se puede plantear el caso de que los documentos secretos se encuentren en un sistema informático. En este supuesto, se aplicaría el criterio de la consunción del delito cuyo umbral típico se ubica más lejos de la afección al bien jurídico protegido y por tanto, en este caso, estando más lejos el artículo 198 CP, el concurso de normas entiendo que se resolvería a favor del artículo 415 CP.

***SEXAGÉSIMA PRIMERA.-*** Por lo que respecta al artículo 536 CP, el artículo 198 CP tiene la peculiaridad de que, en relación con las conductas de *hacking* que nos ocupan, además de requerir el acceso al sistema informático, exigiría que la autoridad o funcionario público actuase "*fuera de los casos permitidos por la Ley*", "*sin mediar causa legal por delito*" y "*prevaliéndose de su cargo*", por lo que en puridad entiendo que no parece que pueda plantearse un concurso de normas.

***SEXAGÉSIMA SEGUNDA.-*** En el caso del artículo 198 CP el precepto contiene un delito especial impropio o alternativa típica agravada por las características del autor. De esta forma, si intervienen varios sujetos, cada uno deberá responder conforme a su hecho y culpabilidad, es decir, conforme al artículo 65 CP, esto significa que la autoridad o funcionario público responderá conforme al artículo 198 CP y quien no tenga esa condición quedará sujeto al artículo 197 *bis* 1 CP.

***SEXAGÉSIMA TERCERA.-*** Con la incorporación del artículo 198 en el CP se pone fin al tratamiento privilegiado para las autoridades o funcionarios públicos que llevaban a cabo injerencias ilegítimas en los derechos y libertades de los ciudadanos, recibiendo ahora un tratamiento agravado respecto al correlativo delito de *hacking*.

***SEXAGÉSIMA CUARTA.-*** En el artículo 198 CP se toma como punto de partida el concepto normativo de autoridad o funcionario público contenido en el artículo 24 CP, si bien matizado jurisprudencialmente al incluir una interpretación del término acorde con cada caso concreto, atendiendo a que el sujeto participe de forma temporal o permanente en funciones públicas, habiendo sido designado para su ejercicio.

***SEXAGÉSIMA QUINTA.-*** Por lo que respecta a la actuación *"fuera de los casos permitidos por la Ley"*, exigida en el tipo agravado, el sujeto obra fuera de sus competencias, como un particular, pero con prevalimiento de la condición especial que ostenta.

***SEXAGÉSIMA SEXTA.-*** Además, el citado precepto exige que no medie causa legal por delito en el acceso al sistema informático, lo que supone que el acceso ilícito al sistema de información no guarde relación con las actividades en un procedimiento en torno a la investigación de un delito.

***SEXAGÉSIMA SÉPTIMA.-*** La existencia del procedimiento judicial o las diligencias policiales serán las que determinen si media causa por delito y por tanto la conducta es encuadrable en el artículo 198, lo que no excluye, que medie causa penal sobre un sujeto y, fuera de esa investigación, se lleve a cabo el acceso a un sistema informático con la correspondiente lesión para su seguridad, supuesto en el que igualmente se aplicaría el artículo 198 CP.

***SEXAGÉSIMA OCTAVA.-*** En el citado tipo agravado los hechos han de producirse con prevalimiento del cargo, circunstancia que, al ser inherente al delito, impide la aplicación de la agravante genérica del artículo 22.7ª CP.

Si la autoridad o funcionario público no se prevaliera de su cargo, aun constando una investigación criminal por delito sobre el sujeto, habría que acudir al tipo común.

***SEXAGÉSIMA NOVENA.-*** Con la introducción de la responsabilidad penal de las personas jurídicas en el intrusismo informático se emplea un nuevo instrumento para la prevención y la persecución de estos delitos, que ya de por sí son suficientemente complejos pero que además están en continua evolución, necesitando por ello el Estado de nuevos mecanismos para asegurar que estas conductas no queden impunes y justificando el castigo penal a la persona jurídica por el acceso ilícito a sistemas informáticos ajenos está justificado.

***SEPTUAGÉSIMA.-*** Como persona jurídica a estos efectos, ante la falta de un concepto positivo, atendidos los instrumentos internacionales y a la delimitación negativa del artículo 31 *quinquies* CP se puede entender toda entidad a la cual el derecho vigente reconoce este estatuto, salvo el Estado, otros organismos públicos que ejercen prerrogativas públicas, las organizaciones internacionales de Derecho público, las Administraciones públicas territoriales e institucionales, los Organismos Reguladores, las organizaciones internacionales de Derecho público, las Agencias y Entidades públicas

Empresariales y las organizaciones que ejerzan potestades públicas de soberanía o administrativas.

***SEPTUAGÉSIMA PRIMERA.-*** El nuevo régimen ya no excluye a los partidos políticos, sindicatos ni sociedades mercantiles Estatales, lo cual resulta razonable por cuanto, aunque tengan asignadas determinadas funciones constitucionales o de interés general, el intrusismo informático no se presenta entre ellas, no concurre motivo alguno para tengan el privilegio de no asumir responsabilidad penal por el *hacking* llevado a cabo por sus agentes, por cuenta de la persona moral y en beneficio de ésta.

***SEPTUAGÉSIMA SEGUNDA.-*** En nuestro ordenamiento el sistema introducido es el de responsabilidad directa de la persona jurídica, de forma autónoma de la persona física, por cuanto el propio artículo 31 *bis* 2 del CP se encarga de diferenciarlos y de establecer la responsabilidad con independencia de que la persona física no sea castigada por el delito.

***SEPTUAGÉSIMA TERCERA.-*** En el artículo 31 *bis* se distingue entre lo que se denominan delitos de directivos y delitos de empleados.

En el caso de los directivos, deberán llevar a cabo el intrusismo informático dentro de su mandato o representación, no comprendiendo las actuaciones fuera de ese ámbito, lo que excluiría los casos de extralimitación, y además en beneficio de la entidad.

En cuanto al delito de *hacking* cometido por personas sujetas a la autoridad de esos directivos, deberá existir un incumplimiento grave de los deberes de supervisión, vigilancia y control, lo que exigirá el análisis caso por caso y acudir a la normativa extrapenal para delimitar esas obligaciones en materia de acceso a sistemas informáticos.

***SEPTUAGÉSIMA CUARTA.-*** Entiendo que el castigo de la persona moral en el delito de *hacking* con independencia de la responsabilidad penal de la persona física se muestra una herramienta adecuada para disuadir a las entidades en la comisión de estos delitos y para que adopten las medidas dirigidas a prevenirlos.

***SEPTUAGÉSIMA QUINTA.-*** Por último, el modelo adoptado en el artículo 31 *bis* CP de exención de responsabilidad penal para la persona jurídica, derivada del delito de intrusismo informático, considero que se fundamenta en la falta de tipicidad que existe en los casos en los que se han adoptado los medios necesarios para impedir el delito. De esta forma, la falta de tipicidad de estas conductas cuando concurren los elementos de exención de responsabilidad penal

determina que no sea la persona jurídica quien deba concurrir al juicio para determinar si ha adoptado las medidas adecuadas o no. Desde el inicio podrá comprobarse que falta la tipicidad, posibilitando así la pronta exoneración de esa responsabilidad.

## ÍNDICE DE DOCUMENTOS

NORMATIVOS

**Internacionales**:

- Convención de las Naciones Unidas contra la Delincuencia Organizada Transnacional, hecha en Nueva York el 15 de noviembre de 2000, disponible en http://www.cinu.mx/minisitio/Trafico_migrantes/Conv_Delincuencia_Org.pdf, y ratificado por España el 21 de febrero de 2002, Instrumento de ratificación publicado en el BOE nº 233, de 29 de septiembre de 2003, disponible en https://www.boe.es/buscar/doc.php?id=BOE-A-2003-18040, consultado el 1 de mayo de 2017.

- "Federal Computer System Protection Act of 1977", de fecha 27 de junio de 1977, está disponible en https://www.congress.gov/search?q=%7B"congress"%3A%5B"95"%5D%2C"source"%3A"legislation"%2C"search"%3A"federal+computer+system+protection+act+of+1977"%7D, consultado el 14 de septiembre de 2016.

- Resolución 55/25 dictada por la Asamblea General de la Naciones Unidas en fecha 15 de noviembre de 2000, disponible en http://www.cinu.mx/minisitio/Trafico_migrantes/Conv_Delincuencia_Org.pdf, consultado el 22 de octubre de 2016.

- Resolución de 24 de octubre de 1995 emitida por el *Federal Networking Council* de Estados Unidos, disponible en https://www.nitrd.gov/fnc/Internet_res.aspx, consultado el 14 de septiembre de 2016.

**Europeos**:

- Acta de 24 de octubre de 2008, de reforma del Código penal polaco, disponible en http://isip.sejm.gov.pl/Download;jsessionid=FB60783149CC47AA518F60891929BACE?id=WDU20082141344&type=1, consultado el 23 de septiembre de 2016.

- Código de infracciones reglamentarias de Alemania, de 19 de febrero de 1987, disponible en https://www.gesetze-im-internet.de/owig_1968/inhalts_bersicht.html, consultado el 24 de abril de 2017.

- Código penal de Alemania, de 15 de mayo de 1871, con sus reformas, disponible en https://www.gesetze-im-internet.de/stgb/, consultado el 20 de septiembre de 2016.

- Código penal de Alemania (versión inglesa), de 15 de mayo de 1871, con sus reformas, disponible en http://www.gesetze-im-internet.de/englisch_stgb/index.html, consultado el 20 de septiembre de 2016.

- Código penal de Austria, de 23 de enero de 1974, disponible en https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=10002296, consultado el 20 de septiembre de 2016.

- Código penal de Bélgica, de 8 de junio de 1867, disponible en http://www.ejustice.just.fgov.be/cgi_loi/loi_a1.pl?DETAIL=1867060801%2FF&caller=list&row_id=1&numero=2&rech=4&cn=1867060801&table_name=LOI&nm=1867060850&la=F&dt=CODE+PENAL&language=fr&fr=f&choix1=ET&choix2=ET&fromtab=loi_all&trier=promulgation&chercher=t&sql=dt+contains++%27CODE%27%26+%27PENAL%27and+actif+%3D+%27Y%27&tri=dd+AS+RANK+&imgcn.x=41&imgcn.y=12#LNK0117, consultado el 20 de septiembre de 2016.

- Código penal de Bulgaria, de 1 de mayo de 1968, incluyendo la reforma introducida en el año 2002 por la SG 92/02, se encuentra en http://www.legislationline.org/documents/action/popup/id/8881/preview, consultado el 20 de septiembre de 2016.

- Código penal de Checoslovaquia, de 29 de noviembre de 1961, disponible en en http://business.center.cz/business/pravo/zakony/trestni_zakon/, consultado el 23 de septiembre de 2016.

- Código penal de Croacia, de 21 de octubre de 1997 disponible en http://narodne-novine.nn.hr/clanci/sluzbeni/1997_10_110_1668.html. Versión inglesa en

http://www.legislationline.org/documents/section/criminal-codes, consultado el 20 de septiembre de 2016.

- Código penal de Dinamarca, de 27 de septiembre de 2005, disponible en https://www.retsinformation.dk/Forms/R0710.aspx?id=2406, y en https://www.unodc.org/tldb/pdf/Denmark_Criminal_Code_2005.pdf, en su versión inglesa, consultado el 21 de septiembre de 2016.

- Código penal de Eslovaquia, de 2 de julio de 2005, disponible en http://www.zakonypreludi.sk/zz/2005-300, consultado el 21 de septiembre de 2016.

- Código penal de Eslovenia, de 27 de agosto de 2004, disponible en http://www2.gov.si/up-rs/2002-2007/jd.nsf/dokumentiweb/D4B6CCF32BB7E8A3C1256F94000A952D?OpenDocument, consultado el 21 de septiembre de 2016.

- Código penal de Estonia, de 6 de junio de 2001, disponible en su versión en inglés en https://www.riigiteataja.ee/en/eli/522012015002/consolide, consultado el 18 de septiembre de 2016.

- Código penal de Finlandia, de 19 de diciembre de 1889 disponible en http://www.finlex.fi/fi/laki/ajantasa/1889/18890039001, consultado el 22 de septiembre de 2016.

- Código penal de Francia, de 22 de julio de 1992, disponible en https://www.legifrance.gouv.fr/affichCode.do;jsessionid=FF09C8C93B99E3673DC98E1F25544C0A.tpdila08v_1?cidTexte=LEGITEXT00

0006070719&dateTexte=20151027, consultado el 22 de septiembre de 2016.

- Código penal de Grecia, de 17 de agosto de 1950, disponible en http://www.ministryofjustice.gr/site/kodikes/%CE%95%CF%85%CF%81%CE%B5%CF%84%CE%AE%CF%81%CE%B9%CE%BF/%CE%A0%CE%9F%CE%99%CE%9D%CE%99%CE%9A%CE%9F%CE%A3%CE%9A%CE%A9%CE%94%CE%99%CE%9A%CE%91%CE%A3/tabid/432/language/el-GR/Default.aspx, consultado el 22 de septiembre de 2016.

- Código penal de Holanda, de 3 de marzo de 1881, disponible en http://wetten.overheid.nl/BWBR0001854/2014-07-01, consultado en fecha 22 de septiembre de 2016.

- Código penal de Hungría, de fecha 13 de julio de 2012, disponible en http://net.jogtar.hu/jr/gen/hjegy_doc.cgi?docid=A1200100.TV, consultado el 22 de septiembre de 2016.

- Código penal de Italia, de 19 de octubre de 1930, reformado, disponible en http://www.diritto.it/codici/titolo/75-codice-penale-dei-delitti-contro-la-persona, consultado el 23 de septiembre de 2016.

- Código penal de Letonia, de 17 de junio de 1998, con sus reformas, disponible en http://likumi.lv/doc.php?id=88966, donde también se incluye su versión en inglés, consultado el 23 de septiembre de 2016.

- Código penal de Lituania, de 26 de septiembre de 2000, disponible, con sus reformas, en

http://www.infolex.lt/portal/start_ta.asp?act=doc&fr=pop&doc=66150, consultado el 23 de septiembre de 2016.

- Código penal de Luxemburgo, de 16 de junio de 1879 se encuentra disponible en http://www.legilux.public.lu/leg/textescoordonnes/codes/code_penal/codepenal.pdf, consultado el 23 de septiembre de 2016.

- Código penal de Malta, de 10 de junio de 1854, disponible en http://www.justiceservices.gov.mt/DownloadDocument.aspx?app=lom&itemid=8574, consultado el 23 de septiembre de 2016.

- Código penal de Polonia, de 6 de junio de 1997, disponible en http://isap.sejm.gov.pl/DetailsServlet?id=WDU19970880553, consultado el 23 de septiembre de 2016.

- Código penal de República Checa, de 8 de enero de 2009, disponible en www.mvcr.cz/soubor/sb011-09-pdf.aspx, consultado el 23 de septiembre de 2016.

- Código penal de Rumanía, de 17 de julio de 2009, disponible en http://legislatie.just.ro/Public/DetaliiDocumentAfis/109854, consultado el 23 de septiembre de 2016.

- Código penal de Suecia, de 21 de diciembre de 1962, disponible en https://www.riksdagen.se/sv/Dokument-Lagar/Lagar/Svenskforfattningssamling/Brottsbalk-1962700_sfs-1962-700/#K4, consultado el 23 de septiembre de 2016.

- Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones, Garantizar el espacio de libertad, seguridad y justicia para los ciudadanos europeos, Plan de acción por el que se aplica el programa de Estocolmo, COM (2010) 171 final, de 20 de abril de 2010, está disponible en http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0171:FIN:es:PDF, consultado el 14 de septiembre de 2016.

- 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» (COM/2009/0149 final), de 30 de marzo de 2009, disponible en http://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:52009DC0149&qid=1441210483706&from=ES, consultado el 18 de septiembre de 2016.

- Comunicación de la Comisión al Parlamento Europeo, al Consejo y al Comité de las Regiones: Hacia una política general de lucha contra la ciberdelincuencia (COM(2007) 267 final, de 22 de mayo de 2007), disponible en http://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=URISERV:l14560&from=ES, consultado el 18 de septiembre de 2016.

- Comunicación de la Comisión al Parlamento Europeo y al Consejo de 22 de noviembre de 2010 “La Estrategia de Seguridad Interior de la

UE en acción: cinco medidas para una Europa más segura (COM(2010) 673 final no publicada en el Diario Oficial)", disponible en http://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=URISERV:jl0050&from=ES, consultado el 18 de septiembre de 2016.

- Comunicación de la Comisión al Parlamento Europeo y al Consejo, "Un espacio de libertad, seguridad y justicia al servicio de los ciudadanos", de fecha 10 de junio de 2009, está disponible en http://www.europarl.europa.eu/intcoop/eurolat/working_group_migration/meetings/27_28_01_2010_brussels/dossier/com%282009%290262_es.pdf, consultado el 14 de septiembre de 2016.

- Comunicación de la Comisión, de 31 de mayo de 2006, «Una estrategia para una sociedad de la información segura - Diálogo, asociación y potenciación» (COM (2006) 251 final - no publicada en el Diario Oficial), disponible en http://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=URISERV:l24153a&from=ES, consultado el 18 de septiembre de 2016.

- Comunicación de la Comisión, de 12 de diciembre de 2006, sobre un Programa Europeo para la Protección de Infraestructuras Críticas (COM (2006) 786 final – Diario Oficial C 126 de 7 de junio de 2007), disponible en http://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=URISERV:l33260&from=ES, consultado el 18 de septiembre de 2016.

- Convenio Europeo sobre Cibercriminalidad, aprobado por el Consejo de Europa el 23 de noviembre de 2001 y suscrito por España el 3 de junio de 2010, publicado en el BOE nº 226, de 17 de septiembre de 2010, disponible en https://www.boe.es/diario_boe/txt.php?id=BOE-A-2010-14221, consultado el 7 de enero de 2017.

- Convenio para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, de 28 de enero de 1981, consultado el 14 de septiembre de 2016 en https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016806c1abd.

- Criminal Damage Act irlandés, Ley para enmendar los delitos de daños materiales y prever disposiciones afines, de fecha 27 de diciembre de 1991 está disponible en http://www.irishstatutebook.ie/eli/1991/act/31/enacted/en/print#sec5, consultado el 22 de septiembre de 2016.

- Decisión Marco 2005/222/JAI del Consejo, de 24 de febrero de 2005, relativa a los ataques contra los sistemas de información, disponible en https://www.boe.es/doue/2005/069/L00067-00071.pdf, consultado el 8 de enero de 2017.

- Decisión Marco 2008/841/JAI del Consejo, de 24 de octubre de 2008,
relativa a la lucha contra la delincuencia organizada, disponible en http://eur-

lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:300:0042:0045:ES:PDF, consultado el 22 de octubre de 2016.

- Decreto Legislativo, de 8 de junio de 2001, nº 231, "Disciplina della responsabilita' amministrativa delle persone giuridiche, delle societa' e delle associazioni anche prive di personalita' giuridica, a norma dell'articolo 11 della legge 29 settembre 2000, n. 300", publicado en la *Gazzetta Ufficiale* nº 140 del 19 de junio de 2001, disponible en http://www.parlamento.it/parlam/leggi/deleghe/01231dl.htm, consultado el 23 de abril de 2017.

- Dictamen del Comité Económico y Social Europeo sobre la «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», de fecha 23 de julio de 2011, (COM(2010) 517 final — 2010/0273 (COD)), disponible en http://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:52011AE0816&from=ES, consultado el 18 de septiembre de 2016.

- Directiva 2002/58/CE del Parlamento Europeo y del Consejo, de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas (Directiva sobre la privacidad y las comunicaciones electrónicas), disponible en http://eur-lex.europa.eu/legal-content/es/ALL/?uri=CELEX:32002L0058, consultado el 14 de septiembre de 2016.

- Directiva 2006/24/CE del Parlamento Europeo y del Consejo, de 15 de marzo de 2006, sobre la conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones y por la que se modifica la Directiva 2002/58/CE, está disponible en http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:105:0054:0063:ES:PDF, consultado el 14 de septiembre de 2016.

- Directiva 2011/36/UE del Parlamento Europeo y del Consejo, de 5 abril de 2011, relativa a la prevención y lucha contra la trata de seres humanos y a la protección de las víctimas y por la que se sustituye la Decisión marco 2002/629/JAI del Consejo, http://eur-lex.europa.eu/legal-content/ES/ALL/?uri=CELEX:32011L0036, consultado el 4 de febrero de 2017.

- Directiva 2013/40/UE del Parlamento Europeo y del Consejo, de 12 de agosto de 2013, relativa a los ataques contra los sistemas de información y por la que se sustituye la Decisión marco 2005/222/JAI del Consejo, disponible en https://www.boe.es/doue/2013/218/L00008-00014.pdf, consultado el 8 de enero de 2017.

- "eEurope 2002 COM/2000/0890", de 26 de enero de 2001, disponible en http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:52000DC0890, consultado el 7 de enero de 2017.

- Informe Bangemann (Bangemann Report), encargado por el Consejo Europeo y emitido el 26 de mayo de 1994, disponible en http://ec.europa.eu/archives/ISPO/infosoc/backg/bangeman.html, consultado el 4 de enero de 2016.

- Informe Statewatch "European Union and FBI launch global surveillance system", de diciembre de 1991, disponible en http://cryptome.org/jya/eu-fbi.htm, consultado el 7 de enero de 2017.

- Ley de abusos informáticos de Reino Unido, de fecha de 29 de junio de 1990, disponible en su texto original en http://www.legislation.gov.uk/ukpga/1990/18/pdfs/ukpga_19900018_en.pdf, y con sus reformas en http://www.legislation.gov.uk/ukpga/1990/18, consultado el 22 de septiembre de 2016.

- Ley de Alemania, de 7 de agosto de 2007, de reforma del StGB alemán disponible en http://www.buzer.de/gesetz/7846/, consultado el 20 de septiembre de 2016.

- Ley de Austria, de 28 de diciembre de 2007 de modificación del Código penal austríaco, disponible en https://www.ris.bka.gv.at/Dokumente/BgblAuth/BGBLA_2007_I_109/BGBLA_2007_I_109.pdf, consultado el 20 de septiembre de 2016.

- Ley de Austria nº 134/2002, de 13 de agosto, de modificación del Código penal austríaco, Ley

disponible en https://www.ris.bka.gv.at/Dokumente/BgblPdf/2002_134_1/2002_134_1.pdf, consultado el 20 de septiembre de 2016.

- Ley de Francia nº 2015-912 de 24 de julio de 2015, relativa a la información, disponible en http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000030931899&categorieLien=id, consultado el 22 de septiembre de 2016.

- Ley de Francia nº 88-19, de 5 de enero de 1988, relativa al fraude informático, disponible en http://www.legifrance.gouv.fr/jopdf/common/jo_pdf.jsp?numJO=0&dateJO=19880106&numTexte=&pageDebut=00231&pageFin=00231, consultado el 22 de septiembre de 2016.

- Ley de Holanda, de 1 de junio de 2006, para enmendar el Código penal, procedimiento penal y otras leyes sobre los nuevos desarrollos en la tecnología de la información (delitos informáticos II) disponible en https://www.eerstekamer.nl/behandeling/20060713/publicatie_wet_2/document3/f=/w26671st.pdf, consultado el 22 de septiembre de 2016.

- Ley de Hungría, de 18 de diciembre de 2001, de reforma de los artículos 300/C y 300/E de su Código Penal de 1978, disponible en http://njt.hu/cgi_bin/njt_doc.cgi?docid=3356, consultado el 22 de septiembre de 2016.

- Ley de Italia nº 547/1993, de 23 de diciembre 1993, de modificación del Código Penal y Código de Procedimiento Penal en materia de

delincuencia informática, disponible en http://www.wipo.int/wipolex/es/text.jsp?file_id=230249, consultado el 23 de septiembre de 2016.

- Ley de Letonia, de 25 de septiembre de 2014, de modificación de su Código penal, disponible en http://likumi.lv/ta/id/269516-grozijumi-kriminallikuma, consultado el 23 de septiembre de 2016.

- Ley de Letonia, de 28 de abril de 2005, de modificación de su Código Penal, disponible en http://likumi.lv/doc.php?id=108357, consultado el 23 de septiembre de 2016.

- Ley de Lituania, de 11 de junio de 2015, de reforma del Código penal lituano, disponible en http://www3.lrs.lt/pls/inter3/oldsearch.preps2?a=1041675&b=, consultado el 23 de septiembre de 2016.

- Ley de Lituania, de 28 de junio de 2007, de reforma del Código penal lituano, disponible en http://www3.lrs.lt/pls/inter3/oldsearch.preps2?a=301997&b=, consultado el 23 de septiembre de 2016.

- Ley de Lituania, de 29 de enero de 2004, de reforma del Código penal lituano, disponible en http://www3.lrs.lt/pls/inter3/oldsearch.preps2?a=226955&b=, consultado el 23 de septiembre de 2016.

- Ley de Luxemburgo, de 18 de julio de 2014, de reforma del Código penal de Luxemburgo, disponible en

http://www.legilux.public.lu/leg/a/archives/2014/0133/a133.pdf, consultado el 23 de septiembre de 2016.

- Ley de Luxemburgo, de 15 de julio de 1993, de reforma del Código penal de Luxemburgo, disponible en http://www.legilux.public.lu/rgl/1993/A/1152/1.pdf, consultado el 23 de septiembre de 2016.

- Ley de Luxemburgo, de 10 de noviembre de 2006, de reforma del Código penal de Luxemburgo, disponible en http://www.legilux.public.lu/rgl/2006/A/3426/A.pdf, consultado el 23 de septiembre de 2016.

- Ley de Portugal de criminalidad informática, de 17 de agosto de 1991, disponible en http://www.pgdlisboa.pt/leis/lei_mostra_articulado.php?nid=151&tabela=lei_velhas&nversao=1&so_miolo=, consultado el 23 de septiembre de 2016.

- Ley de Portugal n.º 59/2007, de 4 de septiembre, de Vigésima terceira alteração ao Código Penal, aprovado pelo Decreto-Lei n.o 400/82, de 23 de Setembro, disponible en https://www.dgs.pt/accao-de-saude-para-criancas-e-jovens-em-risco/legislacao-relacionada/lei-n-592007-de-4-de-setembro.aspx, consultado el 24 de abril de 2017.

- Ley de Portugal n.º 109/2009, de 15 de septiembre de 2009, de transposición de la DM 2005/222/JAI y el Convenio Europeo sobre Cibercriminalidad, aprobado por el Consejo de Europa el 23 de noviembre de 2001, disponible en

http://www.pgdlisboa.pt/leis/lei_mostra_articulado.php?nid=1137&tabela=leis, consultado el 23 de septiembre de 2016.

- Ley de Rumanía nº 161/2003, de 19 de abril de 2003, disponible en http://legislatie.just.ro/Public/DetaliiDocument/71822, consultado el 23 de septiembre de 2016.

- Ley de Suecia, de 26 de abril de 2007, de modificación del Código penal sueco, disponible en https://www.notisum.se/rnp/sls/sfs/20070213.pdf, consultado el 23 de septiembre de 2016.

- Ley que ratifica la Convención del Consejo de Europa contra la delincuencia a través de Internet, de fecha 30 de abril de 2004, disponible en https://www.google.es/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&uact=8&ved=0ahUKEwjaztmDvcfLAhWCdx4KHQMCCl8QFggdMAA&url=http%3A%2F%2Fwww.police.gov.cy%2Fpolice%2Fpolice.nsf%2FAll%2F7CF46652A4E4D9BDC2257A3A003281B2%2F%24file%2Fnomosdiadiktyou.doc&usg=AFQjCNFjsQuaein0zz8HrVoz_EqYp9CKjg, consultado el 20 de septiembre de 2016.

- Libro verde sobre la obtención de pruebas en materia penal en otro Estado miembro y sobre la garantía de su admisibilidad, emitido por la Comisión Europea en fecha 11 de noviembre de 2009, disponible en http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2009:0624:FIN:ES:PDF, consultado el 14 de septiembre de 2016.

- 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 (COM (2010) 517), de 30 de septiembre de 2010, disponible en http://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:52010PC0517&qid=1441210865885&from=ES, consultado el 18 de septiembre de 2016.

- Protocolo (no 1), sobre el cometido de los Parlamentos nacionales en la UE, publicado en el DOUE, n° C 326 de 26 de octubre de 2012, disponible en http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=celex%3A12012E%2FTXT, consultado el 10 de enero de 2017.

- Recomendación (89) nº 9, de 13 de septiembre de 1989 del Consejo de Europa, disponible en https://www.google.es/search?q=Recomendación+núm.+R+(89)+9+sobre+delitos+informáticos&ie=utf-8&oe=utf-8&gws_rd=cr&ei=kCtDVv_2EMWtaa2cjqAI#q=conseil+europe+R+(89)+9, consultado el 23 de septiembre de 2016.

- "Recommendation No. R (95) 13 of the Committee of Ministers to member states concerning problems of criminal procedural law connected with information technology", de 11 de septiembre de 1995, consultado el 7 de enero de 2017 en http://www.coe.int/t/dghl/standardsetting/media/doc/cm/rec%281995%29013_EN.asp.

- "Recommendation of the Council concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data", emitida por la OCDE en fecha 23 de septiembre de 1980 – C(80) 58/FINAL, enmendada en fecha 11 de julio de 2013, consultado el 14 de septiembre de 2016 en http://acts.oecd.org/Instruments/ShowInstrumentView.aspx?InstrumentID=114&InstrumentPID=312&Lang=en&Book=False.

- "Recommendation Rec (2005) 10 of the Committee of Ministers on "special investigation techniques" in relation to serious crimes including acts of terrorism", de 20 de abril de 2005, consultado el 8 de enero de 2017 en https://wcd.coe.int/ViewDoc.jsp?id=849269&Site=CM.

- Resolución del Consejo de 17 de enero de 1995 sobre la interceptación legal de las telecomunicaciones, en *Diario Oficial de la Unión Europea nº C 329*, de 4 de noviembre de 1996, consultado el 7 de enero de 2017 en http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=uriserv:OJ.C_.1996.329.01.0001.01.SPA.

- Sentencia de la Corte de Apelación de París de fecha 30 de octubre de 2002, asunto Kitetoa, disponible en http://www.kitetoa.com/Pages/Textes/Les_Dossiers/Tati_versus_Kitetoa/arret-cour-appel.shtml, consultado el 22 de septiembre de 2016.

- Tratado de Funcionamiento de la Unión Europea (Versión consolidada), publicada en el DOUE nº C 326 de 26 de octubre de

2012, disponible en http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=celex%3A12012E%2FTXT, consultado el 9 de enero de 2017.

**Nacionales**:

- Anteproyecto de LO por la que se modifica la LO 10/1995, de 23 de noviembre, del Código Penal, aprobado por el Consejo de Ministros el 23 de julio de 2009, disponible en http://www.juecesdemocracia.es/LegislacionActual/CP_Antepro_23_07_09.pdf, consultado el 7 de octubre de 2016.

- Anteproyecto de octubre de 2012, de Ley Orgánica por la que se modifica la LO 10/1995, de 23 de noviembre, del Código Penal, disponible en http://www.mjusticia.gob.es/cs/Satellite/Portal/1292358725605?blobheader=application%2Fpdf&blobheadername1=Content-Disposition&blobheadername2=Medios&blobheadervalue1=attachment%3B+filename%3DAnteproyecto_de_Ley_de_Reforma_del_Codigo_Penal.pdf&blobheadervalue2=1288777317612, consultado el 18 de septiembre de 2016.

-Circular 1/2016 de la FGE, de 22 de enero de 2016, sobre la responsabilidad penal de las personas jurídicas conforme a la reforma del Código Penal efectuada por Ley Orgánica 1/2015, p. 35, disponible en https://www.fiscal.es/fiscal/PA_WebApp_SGNTJ_NFIS/descarga/CI

RCULAR%201-2016%20-%20PERSONAS%20JURÍDICAS.pdf?idFile=cc42d8fd-09e1-4f5b-b38a-447f4f63a041, consultado el 24 de enero de 2017.

- Dictamen de la Comisión de Justicia del Senado emitido en fecha 3 de marzo de 2015 en relación al Proyecto de Ley Orgánica por la que se modifica la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal, disponible en http://www.congreso.es/portal/page/portal/Congreso/PopUpCGI?CMD=VERLST&BASE=pu10&FMT=PUWTXDTS.fmt&DOCS=1-1&DOCORDER=LIFO&QUERY=%28BOCG_D_10_485_3263.CODI.%29#%28P%C3%A1gina6%29, consultado el 18 de septiembre de 2016.

- Dictamen de la Comisión y escritos de mantenimiento de enmiendas fecha 16 de enero de 2015 para su defensa ante el Pleno del Congreso en relación con el Proyecto de Ley Orgánica por la que se modifica la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal, disponible en http://www.congreso.es/portal/page/portal/Congreso/PopUpCGI?CMD=VERLST&BASE=pu10&FMT=PUWTXDTS.fmt&DOCS=1-1&DOCORDER=LIFO&QUERY=%28BOCG-10-A-66-4.CODI.%29#%28P%C3%A1gina1%29, consultado el 18 de septiembre de 2016.

- Dictamen del Consejo de Estado de fecha 27 de junio de 2013, sobre el Anteproyecto de ley orgánica por la que se modifica la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal, disponible

en https://www.boe.es/buscar/doc.php?id=CE-D-2013-358, consultado el 18 de septiembre de 2016.

- Enmiendas al Proyecto de Ley Orgánica por la que se modifica la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal, publicado en el BOCG de 4 de octubre de 2016, disponible en http://www.congreso.es/portal/page/portal/Congreso/PopUpCGI?CMD=VERLST&CONF=BRSPUB.cnf&BASE=PU10&PIECE=PUWD&DOCS=1-1&FMT=PUWTXDTU.fmt&OPDEF=Y&QUERY=BOCG-10-A-66-2.CODI., consultado el 18 de septiembre de 2016.

- Enmiendas de fecha 10 de febrero de 2015, propuestas por el Senado al Proyecto de Ley Orgánica por la que se modifica la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal, disponibles en http://www.congreso.es/portal/page/portal/Congreso/PopUpCGI?CMD=VERLST&BASE=pu10&FMT=PUWTXDTS.fmt&DOCS=1-1&DOCORDER=LIFO&QUERY=%28BOCG_D_10_475_3158.CODI.%29#%28P%C3%A1gina85%29 consultado el 18 de septiembre de 2016.

- Enmiendas y diarios de sesiones al Proyecto de Ley Orgánica por la que se modifica el Código Penal, publicada en el BOCG de 27 de noviembre de 2009, hasta la aprobación de la LO 5/2010, disponible en http://www.congreso.es/portal/page/portal/Congreso/Congreso/Iniciativas?_piref73_2148295_73_1335437_1335437.next_page=/wc/servidorCGI&CMD=VERLST&BASE=IWI9&FMT=INITXDSS.fmt&DOC

S=1-
1&DOCORDER=FIFO&OPDEF=ADJ&QUERY=%28121%2F0000
52*.NDOC.%29, consultado el 18 de septiembre de 2016.

- Informe de la Comisión de estudios e informes del CGPJ emitido en fecha 18 de febrero de 2009, al Anteproyecto de LO por la que se modifica el CP, disponible en http://www.aelpa.org/actualidad/julio2009/Informa%20CP-%20CGPJ.doc, consultado el 4 de octubre de 2016.

- Informe de la Ponencia del Congreso de fecha 13 de enero de 2015, sobre el Proyecto de Ley Orgánica por la que se modifica la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal, disponible en
http://www.congreso.es/portal/page/portal/Congreso/PopUpCGI?CMD=VERLST&BASE=pu10&FMT=PUWTXDTS.fmt&DOCS=1-1&DOCORDER=LIFO&QUERY=%28BOCG-10-A-66-3.CODI.%29#%28P%C3%A1gina1%29, consultado el 18 de septiembre de 2016.

- Informe de la Ponencia del Senado emitido en fecha 23 de febrero de 2015 en relación al Proyecto de Ley Orgánica por la que se modifica la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal, disponible en
http://www.congreso.es/portal/page/portal/Congreso/PopUpCGI?CMD=VERLST&BASE=pu10&FMT=PUWTXDTS.fmt&DOCS=1-1&DOCORDER=LIFO&QUERY=%28BOCG_D_10_481_3237.CO

DI.%29#%28P%C3%A1gina3%29, consultado el 18 de septiembre de 2016.

- Informe del CGPJ de 16 de enero de 2013, al Anteproyecto de Ley Orgánica por la que se modifica la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal, disponible en http://www.poderjudicial.es/cgpj/es/Poder-Judicial/Consejo-General-del-Poder-Judicial/Actividad-del-CGPJ/Informes/Informe-al-Anteproyecto-de-Ley-Organica-por-la-que-se-modifica-la-Ley-Organica-10-1995--de-23-de-noviembre--del-Codigo-Penal, consultado el 18 de septiembre de 2016.

- Informe del Consejo de Estado sobre la Inserción del Derecho europeo en el ordenamiento español, de fecha 14 de febrero de 2008, disponible en http://www.consejo-estado.es/pdf/europa.pdf, consultado el 9 de enero de 2017.

- Informe del Consejo Fiscal al Anteproyecto de Ley Orgánica por la que se modifica la Ley Orgánica 10/1995, de 24 de noviembre (sic), del Código Penal, de 8 de enero de 2013, disponible en https://www.fiscal.es/fiscal/PA_WebApp_SGNTJ_NFIS/descarga/INFORME_ANTEPROYECTO_CP_2012_8-enero-2013.pdf?idFile=ab37a28b-9fbc-4af5-b2b3-3b14c1826623, consultado el 18 de septiembre de 2016.

- Informe del CGPJ al Anteproyecto de 2006 de Ley Orgánica por la que se modifica la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal, se encuentra disponible en

http://www.juecesdemocracia.es/cgpj/2006/octubre/020de.06.pdf, consultado el 18 de septiembre de 2016.

- LO 1/2015, de 30 de marzo, por la que se modifica la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal, publicada en el BOE nº 77, de 31 de marzo de 2015, disponible en https://www.boe.es/diario_boe/txt.php?id=BOE-A-2015-3439, consultado el 18 de septiembre de 2016.

- LO 5/2010, de 22 de junio, por la que se modifica la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal, disponible en http://www.boe.es/boe/dias/2010/06/23/pdfs/BOE-A-2010-9953.pdf, consultado el 18 de septiembre de 2016.

- LO 7/2012, de 27 de diciembre, por la que se modifica la LO 10/1995, de 23 de noviembre, del Código Penal en materia de transparencia y lucha contra el fraude fiscal y en la Seguridad Social, publicada en el BOE de 28 de diciembre de 2012, disponible en http://www.boe.es/diario_boe/txt.php?id=BOE-A-2012-15647, consultado el 27 de enero de 2017.

- Proyecto de Ley Orgánica por la que se modifica la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal, publicado el 15 de enero de 2007 en el BOCG, disponible en http://www.congreso.es/public_oficiales/L8/CONG/BOCG/A/A_119-01.PDF, consultado el 18 de septiembre de 2016.

- Proyecto de Ley Orgánica por la que se modifica la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal, publicado el 27 de

noviembre de 2009 en el BOCG, núm. 52-1, disponible en http://www.congreso.es/public_oficiales/L9/CONG/BOCG/A/A_052-01.PDF#page=1, consultado el 18 de septiembre de 2016.

- Proyecto de Ley Orgánica por la que se modifica la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal, publicado el 4 de octubre de 2016 en el BOCG, disponible en http://www.congreso.es/public_oficiales/L10/CONG/BOCG/A/BOCG-10-A-66-1.PDF#page=1, consultado el 18 de septiembre de 2016.

- Texto aprobado por el Pleno del Congreso de los Diputados, relativo al Proyecto de Ley Orgánica por la que se modifica la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal, con entrada en el Senado el 29 de enero de 2015, disponible en http://www.congreso.es/portal/page/portal/Congreso/PopUpCGI?CMD=VERLST&BASE=pu10&FMT=PUWTXDTS.fmt&DOCS=1-1&DOCORDER=LIFO&QUERY=%28BOCG_D_10_465_3148.CODI.%29#%28P%C3%A1gina2%29, consultado el 18 de septiembre de 2016.

- Texto aprobado por el Pleno del Senado en fecha 11 de marzo de 2015 en relación al Proyecto de Ley Orgánica por la que se modifica la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal, disponible en http://www.congreso.es/portal/page/portal/Congreso/PopUpCGI?CMD=VERLST&BASE=pu10&FMT=PUWTXDTS.fmt&DOCS=1-1&DOCORDER=LIFO&QUERY=%28BOCG_D_10_493_3340.CO

DI.%29#%28P%C3%A1gina2%29, consultado el 18 de septiembre de 2016.

- Texto del Proyecto de Ley Orgánica por la que se modifica la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal, aprobado por el Pleno del Congreso de los Diputados el 21 de enero de 2015, disponible en http://www.congreso.es/portal/page/portal/Congreso/PopUpCGI?CMD=VERLST&BASE=pu10&FMT=PUWTXDTS.fmt&DOCS=1-1&DOCORDER=LIFO&QUERY=%28BOCG-10-A-66-5.CODI.%29#%28P%C3%A1gina1%29, consultado el 18 de septiembre de 2016.

- Texto del Proyecto de Ley Orgánica por la que se modifica la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal, aprobado por el Congreso de los en fecha 26 de marzo de 2015, disponible en http://www.congreso.es/portal/page/portal/Congreso/PopUpCGI?CMD=VERLST&BASE=pu10&FMT=PUWTXDTS.fmt&DOCS=1-1&DOCORDER=LIFO&QUERY=%28BOCG_D_10_493_3340.CODI.%29#%28P%C3%A1gina2%29, consultado el 18 de septiembre de 2016.

NO NORMATIVOS

**Internacionales**:

- Historia del Centro de ordenadores de la conocida hoy como Universidad Concordia está disponible en su página web: http://archives.concordia.ca/fr/node/1695, consultado el 14 de septiembre de 2016.

- Lista de estadísticas Kaspersky del año 2016 sobre ataques maliciosos contados en 212 países y neutralizados por sus productos. Disponible en https://go.kaspersky.com/LATAM_Security_Bulletin_2016_Stats_SP_SOC_2016.html consultado el 5 de enero de 2017.

- Manual de las Naciones Unidas sobre prevención y control de delitos informáticos, Revista Internacional de Política Criminal, Números 43 y 44, 1994, consultado el 14 de septiembre de 2016 en https://www.google.es/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=0CCkQFjAA&url=https%3A%2F%2Fcms.unov.org%2FDocumentRepositoryIndexer%2FGetDocInOriginalFormat.drsx%3FDocID%3Dd387f5c7-8c0d-41ad-b354-a154c3de1f8d&ei=tMSWU8aJJKWX1AW0rQE&usg=AFQjCNH7Qm-EH-Nw78upQ6fVxKEnCb5CQw&bvm=bv.68445247,d.d2k&cad=rja.

- Octavo Congreso de las Naciones Unidas sobre Prevención del Delito y Tratamiento del Delincuente, A/RES/45/121, de fecha 14 de diciembre de 1990, disponible en

http://www.un.org/documents/ga/res/45/a45r121.htm, consultado el 7 de enero de 2017.

**Europeos**:

- Firmas, ratificaciones, declaraciones, reservas, comunicaciones, resumen e informe explicativo del Convenio Europeo sobre Cibercriminalidad, aprobado por el Consejo de Europa el 23 de noviembre de 2001, disponible en http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=185&CM=8&DF=&CL=ENGconsultado el 16 de septiembre de 2016.

- Lista de Estados firmantes del Convenio Europeo sobre Cibercriminalidad, aprobado por el Consejo de Europa el 23 de noviembre de 2001, disponible en http://www.coe.int/es/web/conventions/full-list/-/conventions/treaty/185/signatures?p_auth=LdzvnXOk, consultado el 22 de septiembre de 2016.

- Lista de Estados miembros de la Unión Europea y su año de ingreso, disponibles en http://europa.eu/about-eu/countries/index_es.htm, consultado el 20 de septiembre de 2016.

**Nacionales**:

- Referencia del Consejo de Ministros de fecha 14 de julio de 2006 a la recepción del Informe del Ministro de Justicia sobre el

Anteproyecto de Ley Orgánica por la que se modifica la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal, disponible en http://www.lamoncloa.gob.es/consejodeministros/referencias/Paginas/2006/refc20060714.aspx#C%C3%B3digoPenal, consultado el 18 de septiembre de 2016.

## JURISPRUDENCIA CONSULTADA

TRIBUNALES ESPAÑOLES:

**Tribunal Constitucional:**

- STC 22/1984, Sala Segunda, de 17 de febrero de 1984, Recurso 59/1983, Pte. Excmo. Sr. D. Luis Díez-Picazo y Ponce de León (EDJ 1984/22).
- STC 20/1992, Sala Primera, de 14 de febrero de 1992, Recurso 1696/1988, Pte. Excmo. Sr. D. Francisco Tomás y Valiente (RTC 1992\20).
- STC 254/1993, Sala Primera, de 20 de julio de 1993, Recurso de Amparo núm. 1827/1990, Pte. Ilmo. Sr. D. Fernando García-Mon y González Regueral (RTC 1993\254).
- STC 143/1994, Sala Primera, de 9 de mayo de 1994, Recurso de Amparo núm. 3192/1992, Pte. Ilmo. Sr. D. Miguel Rodríguez-Piñero y Bravo-Ferrer (RTC 1994\143).
- STC 290/2000, Pleno, de 30 de noviembre de 2000, Recurso de Inconstitucionalidad núms. 201/1993, 219/1993, 226/1993 y 236/1993, Pte. Ilmo. Sr. D. Julio Diego González Campos (RTC 2000\290).
- STC 292/2000, Pleno, de 30 de noviembre de 2000, Recurso de Amparo núm. 1463/2000, Pte. Ilmo. Sr. D. Julio Diego González Campos (RTC 2000\292).

- STC 196/2004, Sala Primera, de 15 de noviembre de 2004, Recurso 1322/2000, Pte. Excmo. Sr. D. Francisco Javier Delgado Barrio (EDJ 2004/157278).
- STC 206/2007, Sala Primera, de 24 de septiembre de 2007, Recurso 4487/2005, Pte. Excmo. Sr. D. Manuel Aragón Reyes (EDJ 2007/158668).
- STC 209/2007, Sala Primera, de 24 de septiembre de 2007, Recurso 6377/2005, Pte. Excma. Sra. Dª María Emilia Casas Baamonde (EDJ 2007/174423).
- STC 159/2009, Sala Segunda, de 29 de junio de 2009, Recurso 9914/2006, Pte. Excmo. Sr. D. Vicente Conde Martín de Hijas (EDJ 2009/150475).
- STC 70/2009, Sala Primera, de 23 de marzo de 2009, Recurso 2826/2004, Pte. Excma. Sra. Dª María Emilia Casas Baamonde (EDJ 2009/50401).
- STC 173/2011, de 7 de noviembre de 2011, Recurso de Amparo núm. 5928/2009, Ponente Ilmo. Sr. D. Eugeni Gay Montalvo (RTC 2011\173).

**<u>Tribunal Supremo</u>:**

- STS, Sala de lo Criminal, de 7 de junio de 1985, Pte. Excmo. Sr. D. Luis Vivas Marzal, (RJ 1985\2973).
- STS, Sala Segunda, de 14 de septiembre de 1989, Pte. Excmo.

Sr. D. Francisco Soto Nieto (RJ 1989\6644).

- STS, Sala Segunda, de 21 de mayo de 1990, Pte. Excmo. Sr. D. Luis Vivas Marzal, (RJ 1990\4202).
- STS, Sala Segunda, de 6 de julio de 1990, Pte. Excmo. Sr. D. Francisco Soto Nieto (RJ 1990/6254).
- STS, Sala Segunda, de 11 de octubre de 1993, nº 2208/1993, recurso 3286/1989, Pte. Excmo. Sr. D. Justo Carrero Ramos (RJ 1993\7705).
- STS, Sala Segunda, nº 178/1996, de 1 de marzo de 1996, Recurso de Casación núm. 2144/1995, Pte. Ilmo. D. José Antonio Martín Pallín (RJ 1996\1886).
- STS, Sala Segunda, nº 234/1999, de 18 de febrero de 1999, Recurso de Casación núm. 3256/1998, Pte. Ilmo. Sr. D. José Jiménez Villarejo (EDJ 1999/377 y RJ 1999\510).
- STS, Sala Segunda, de 11 de julio de 2001, nº 1461/2001, recurso 3323/1999, Pte. Excmo. Sr. D. José Ramón Soriano Soriano (EDJ 2001/16167)
- STS, Sala Segunda, de 29 de noviembre de 2002, nº 1994/2002, recurso 1621/2001, Pte. Excmo. Sr. D. José Ramón Soriano Soriano (RJ 2002\10874).
- STS, Sala Segunda, de 20 de junio de 2003, nº 694/2003, recurso 2667/2001, Pte. Ilmo. Sr. D. Eduardo Móner Muñoz (RJ 2003\4359).
- STS, Sala Segunda, de 11 de junio de 2004, nº 725/2004,

recurso 471/2003, Pte. Excmo. Sr. D. Enrique Bacigalupo Zapater (EDJ 2004/82679).

- STS, Sala Segunda, de 10 de diciembre de 2004, nº 1444/2004, recurso 2385/2003, Pte. Excmo. Sr. D. José Manuel Maza Martín (RJ\2005\879).
- STS, Sala Segunda, de 23 de mayo de 2005, nº 663/2005, Pte. Excmo. Sr. D. Juan Ramón Berdugo y Gómez de la Torre (RJ 2005\7339).
- STS, Sala Segunda, de 10 de noviembre de 2005, nº 1315/2005, Pte. Excmo. Sr. D. Juan Ramón Berdugo y Gómez de la Torre (RJ 2006\3099).
- STS, Sala Segunda, de 19 de junio de 2006, nº 666/2006, Pte. Excmo. Sr. D. Perfecto Andrés Ibáñez (RJ 2006\4929).
- STS, Sala Segunda, de 20 de septiembre de 2006, nº 913/2006, recurso 1854/2005, Pte. Excmo. Sr. D. José Antonio Martín Pallín (RJ\2006\6401).
- STS, Sala Segunda, de 21 de marzo de 2007, nº 237/2007, recurso 2051/2005, Pte. Ilmo. Sr. D. Miguel Colmenero Menéndez de Luarca (EDJ 2007/18004).
- STS, Sala Segunda, de 30 de abril de 2007, nº 358/2007, recurso 1805/2006, Pte. Ilmo. Sr. D. Miguel Colmenero Menéndez de Luarca (RJ 2007\3724).
- STS, Sala Segunda, de 10 de diciembre de 2007, nº 1122/2007,

recurso 576/2007, Pte. Excmo. Sr. D. Francisco García Pérez (RJ 2007\9120).

- STS, Sala Segunda, de 5 de febrero de 2008, nº 44/2008, recurso 1208/2007, Pte. Excmo. Sr. D. Enrique Bacigalupo Zapater, FJ 2º (RJ 2008\1723).

- STS, Sala Segunda, de 3 de febrero de 2009, nº 123/2009, recurso 1462/2007, Pte. Excmo. Sr. D. Luciano Varela Castro (EDJ 2009/50757).

- ATS, Sala Segunda, de 14 de mayo de 2009, nº 1114/2009, Pte. Excmo. Sr. D. Adolfo Prego de Oliver y Tolivar (JUR 2009\267915).

- STS, Sala Segunda, de 2 de noviembre de 2011, nº 1125/2011, recurso 972/2011, Pte. Excmo. Sr. D. Juan Ramón Berdugo y Gómez de la Torre, (RJ 2012\1380).

- STS, Sala Segunda, de 3 de mayo de 2013, nº 377/2013, recurso 1041/2012, Pte. Excmo. Sr. D. Miguel Colmenero Menéndez de Luarca (EDJ 2013/55362).

- STS, Sala Segunda, de 8 de octubre de 2013, nº 703/2013, recurso 10263/2013, Pte. Excmo. Sr. D. Juan Ramón Berdugo y Gómez de la Torre, FJ 8º, (RJ 2014\424).

- STS, Sala Segunda, de 17 de junio de 2014, nº 525/2014, nº 525/2014, Pte. Excma. Sra. Dª Ana María Ferrer García (RJ 2014\4513).

- STS, Sala Segunda, de 22 de diciembre de 2014, nº 877/2014, recurso 10636/2014, Pte. Excmo. Sr. D. Juan Ramón Berdugo y Gómez de la Torre (RJ\2014\6661).

- STS, Sala Segunda, de 4 de febrero de 2015, nº 23/2015, recurso 10144/2014, Pte. Excmo. Sr. D. Juan Ramón Berdugo y Gómez de la Torre (RJ 2015\2792).

- STS, Sala Segunda, de 24 de febrero de 2015, nº 97/2015, recurso 1774/2014, Pte. Excmo. Sr. D. Juan Ramón Berdugo y Gómez de la Torre (EDJ 2015/26815).

- STS, Sala Segunda, de 16 de marzo de 2015, nº 155/2015, recurso 1589/2014, Pte. Excmo. Sr. D. Alberto Jorge Barreiro, FJ 2º (RJ 2015\1142).

- STS, Sala Segunda, de 10 de julio de 2015, nº 454/2015, recurso 10746/2014, Pte. Excmo. Sr. D. Juan Ramón Berdugo y Gómez de la Torre (RJ\2015\6558).

- STS, Sala Segunda, de 23 de septiembre de 2015, nº 534/2015, recurso 462/2015, Pte. Excmo. Sr. D. Miguel Colmenero Menéndez de Luarca (EDJ 2015/168056).

- STS, Sala 2ª, de 29 de febrero de 2016, nº 154/2016, recurso 10011/2015, Pte. Excmo. Sr. D. José Manuel Maza Martín.

- STS, Sala 2ª, de 16 de marzo de 2016, nº 221/2016, recurso 1535/2015, Pte. Excmo. Sr. D. Manuel Marchena Gómez.

- STS, Sala Segunda, de 21 de junio de 2016, nº 544/2016, Pte. Excmo. Sr. D. Juan Ramón Berdugo y Gómez de la Torre (RJ 2016\2834).

- STS, Sala 2ª, de 27 de julio de 2016, nº 693/2016, recurso 10896/2015, Pte. Excmo. Sr. D. José Manuel Maza Martín (EDJ 2016/113593).

**Audiencia Nacional**:

- SAN, Sala de lo Penal, nº 51/2014, de 3 de noviembre de 2014, Pte. Ilmo. Sr. D. Nicolás Poveda Peñas (JUR 2014\283335).

**Audiencias Provinciales:**

- SAP de Guipúzcoa nº 31/2000, de 21 de marzo, Pte. Ilmo. Sr. D. José Luis Barragán Morales (ARP 2000, 59).
- SAP de Tarragona de 23 de julio de 2001, recurso 735/2000, Pte. Ilmo. Sr. D. Xavier Nouvilas Puig (EDJ 2001/43367).

- SAP de Lleida nº 90/2004, de 25 de febrero de 2004, Pte. Ilmo. Sr. D. Luis Fernando Ariste López (ARP\2004\636).

- SAP de Madrid nº 574/2005, de 25 de mayo de 2005, Pte. Ilma. Sra. Dª Matilde Guerrera Roig (EDJ 2005/73636).

- SAP de Palencia nº 32/2006, de 28 de junio de 2006, Recurso

de Apelación nº 33/2006, Pte. Ilmo. Sr. D. Mauricio Bugidos San José (JUR\2006\248489).

- SAP de Barcelona nº 72/2008, de 18 de enero de 2008, Recurso de Apelación núm. 166/2007, Pte. IIlma. Sra. Dª Bibiana Segura Cros (JUR\2008\106746).

- SAP de Santa Cruz de Tenerife nº 791/2008, de 7 de noviembre de 2008, Recurso de Apelación núm. 232/2008, Pte. Ilmo. Sr. D. Joaquín Luis Astor Landete (EDJ 2008/331639 y JUR 2009\120011).

- SAP de Albacete nº 236/2009, de 27 de octubre de 2009, Recurso de Apelación 134/2009, Pte. Ilma. Sra. Dª Mª Angeles Montalvá Sempere (EDJ 2009/283500).

- SAP de Valladolid, Sección 4ª, de 18 de marzo de 2011, nº 102/2011, recurso 52/2011, Pte. Ilmo. Sr. D. José Luis Ruiz Romero (JUR 2011\155178).

- SAP de Asturias nº 184/2010, de 1 de septiembre de 2010, Pte. Ilma. Sra. Dª Ana Álvarez Rodríguez (ARP 2010\1177).

- SAP de Sevilla, Sección 7ª, de 7 de diciembre de 2011, nº 76/2011, recurso nº 6122/2011, Pte. Ilmo. Sr. D. Francisco Javier González Fernández (ARP 2012\151).

- SAP de Valencia, Sección 3ª, de 4 de mayo de 2012, nº 335/2012, recurso 89/2011, Pte. Ilma. Sra. Dª Lucía Sanz Díaz (JUR 2012\286929).

- SAP de Madrid, Sección 2ª, de 17 de julio de 2012, nº 402/2012, recurso 134/2012, Pte. Ilma. Sra. Dª María del Rosario Esteban Meilan (JUR 2012\282265).

- Auto de la Ilma. Audiencia Provincial de Barcelona, de 22 de octubre de 2012, nº 784/2012, recurso 511/2012, Pte. Ilma. Sra. Dª Elena Guinduláin Oliveras (JUR 2012\372378).

- SAP de Barcelona nº 155/2014, Seccion 8ª, de 19 de febrero de 2014, Pte. Ilmo. Sr. D. Jesús María Barrientos Pacho (JUR 2014\84549).

- SAP de Vizcaya, Sección 2ª, de 23 julio de 2014, nº 90307/2014, recurso nº 143/2014, Pte. IIlmo. Sr. D. Manuel Ayo Fernández (JUR 2014\267848).

- SAP de Girona, Sección 4ª, de 22 de septiembre de 2014, nº 504/2014, Pte. Ilmo. Sr. D. Adolfo García Morales (JUR 2015\43164).

- SAP de Murcia, Sección 3ª, de 20 de febrero de 2015, nº 88/2015, recurso 184/2014, Pte. Ilmo. Sr. D. Juan del Olmo Gálvez.

- SAP de Alicante, Sección 10ª, de 16 de septiembre de 2015, nº 351/2015, Pte. Ilmo. Sr. D. Javier Martínez Marfil (JUR 2016\133547).

**Juzgados:**


- Sentencia del Juzgado de lo Penal 2 de Barcelona de 28 de mayo de 1999, Procedimiento Abreviado 130/99-E, Pte. Ilmo. Sr. D. Juan Carlos Llavona Calderón, en http://www.bufetalmeida.com/58/caso-hispahack-1-absolucion-de-presuntos-hackers-la-sentencia.html consultado el 23 de febrero de 2012.

- Auto del Juzgado de Instrucción 2 de Lorca, de 29 de enero de 2002, Procedimiento Abreviado 1527/99, Pte. Ilmo. Sr. D. Antonio Alcazar Fajardo, en http://documentostics.com/component/option,com_docman/task,doc_view/gid,700/ el 23 de febrero de 2012.

- Sentencia del Juzgado de lo Penal 2 de Badajoz 42/2006, de 15 de febrero de 2006, Pte. Ilmo. Sr. D. Emilio Francisco Serrano Molerá, (EDJ 2006/21611).

- Sentencia del Juzgado de lo Penal 11 de Barcelona, de 20 de julio de 2008, Pte. Ilma. Sra. Dª María Gabriela Boldo Prats (EDJ 2008/138308).

- Sentencia del Juzgado de lo Penal 1 de Oviedo 120/2010, de 23 de marzo de 2010, Pte. Ilmo. Sr. D. José María Serrano Alonso (Fondo Documental CENDOJ).

TRIBUNALES EXTRANJEROS:


- Sentencia del Tribunal Supremo de Estados Unidos Reno vs. American Civil Liberties Union, de 26 de junio de 1997, disponible en http://caselaw.lp.findlaw.com/cgi-bin/getcase.pl?court=us&navby=case&vol=521&invol=844, consultado en 13 de septiembre de 2016.
- Sentencia 1675/2000 de la Corte Suprema de Casación italiana, Sección Quinta, de fecha 7 de noviembre de 2000, disponible en http://www.penale.it/giuris/cass_011.htm, consultado el 4 de octubre de 2016.
- Sentencia de la Corte de Apelación de París de fecha 30 de octubre de 2002, asunto Kitetoa.
- Sentencia del Tribunal de Casación italiano, Sección Conjunta, de 27 de octubre de 2011, disponible en http://www.penale.it/page.asp?IDPag=1021, consultado el 29 de octubre de 2016.

## BIBLIOGRAFÍA CONSULTADA


ÁLVAREZ GARCÍA, F. J., GONZÁLEZ CUSSAC, J. L. (Dir.) y VVAA, *Comentarios a la Reforma Penal de 2010,* ed. Tirant Lo Blanch, Valencia, 2010.

ALONSO GARCÍA, J., "Tratamiento penal del espionaje informático", en *Revistaiuris*, diciembre, nº 155, 2010, consultado el 28 de marzo de 2012 en http://www.revistaiuris.com/ver_detalleArt.asp?idArt=65026&action=detalle.

ALONSO GARCÍA, J., *Derecho penal y redes sociales*, ed. Thomson Reuters Aranzadi, primera edición, Navarra, 2015.

ÁLVAREZ VIZCAYA, M., "Consideraciones político criminales sobre la delincuencia informática: el papel del Derecho penal en la red", en *Internet y Derecho penal. Cuadernos de Derecho Judicial*, Madrid, 2001.

ANARTE BORRALLO, E., "Incidencia de las nuevas tecnologías en el sistema penal", en *Derecho y conocimiento: anuario jurídico sobre la sociedad de la información y del conocimiento*, nº 1, ed. Facultad de Derecho de la Universidad de Huelva, Huelva, 2001.

ANARTE BORRALLO, E., "Sobre los límites de la protección penal de datos personales", en *Derecho y conocimiento: anuario jurídico sobre la sociedad de la información y del conocimiento*, nº

2, ed. Facultad de Derecho de la Universidad de Huelva, Huelva, 2002.

ANARTE BORRALO, E., MORENO MORENO, F. y GARCÍA RÚIZ, C. (Coordinadores), *Nuevos conflictos sociales. El papel de la privacidad*, ed. Iustel, Madrid, 2015.

ANARTE BORRALLO, E. y DOVAL PAÍS, A., "Delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio (1). Delitos contra la intimidad y los datos personales", en BOIX REIG, J. (Dir.) y VVAA, *Derecho Penal. Parte Especial. Volumen I. La protección penal de los intereses jurídicos personales (adaptado a las reformas de 2010 del Código penal)*, ed. Iustel, primera edición, Madrid, 2010.

ANARTE BORRALLO, E. y DOVAL PAIS, A., "Límites de la ley penal a propósito del nuevo delito de intrusión informática", en *RGDP*, noviembre 2012, nº 18.

ANARTE BORRALLO, E. y DOVAL PAIS, A., "Delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio (1). Delitos contra la intimidad y los datos personales", en BOIX REIG, J. (Dir.) y VVAA, *Derecho Penal. Parte Especial. Volumen I. La protección penal de los intereses jurídicos personales*, ed. Iustel, segunda edición, Madrid, 2016.

ANARTE BORRALLO, E y DOVAL PAÍS, A., "Efectos de la reforma de 2015 en los delitos contra la intimidad", en *Diario La Ley*, nº 8744, 19 de abril de 2016.

ANTOLISEI, F., *Manual de Derecho Penal. Parte General*, ed. Temis, Bogotá 1988, traducida por GUERRERO, J., y AYERRA REDÍN, M.

ANTÓN ONECA, J., *Derecho Penal*, ed. Akal, segunda edición, anotada y corregida por HERNÁNDEZ GUIJARRO, J.J. y BENEYTEZ MERINO, L., Madrid, 1986.

ARMAZA ARMAZA, E. J. (Coord.), y VVAA, *La adaptación del Derecho penal al desarrollo social y tecnológico*, ed. Comares, Granada, 2010.

BACIGALUPO SAGGESSE, S., "Artículo 31 y 31 *bis*", en GÓMEZ TOMILLO, M. (Dir.) y VVAA, *Comentarios al Código Penal*, ed. Lex Nova, primera edición, Valladolid, 2010.

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)", *Diario La Ley on-line*, nº 7541, de 5 de enero de 2011, ed. La Ley, Madrid.

BAIO, A., "Pervading animal and Elk Cloner", en *Waxi*, 3 de agosto de 2003, consultado el 14 de septiembre de 2016 en http://waxy.org/2003/08/pervading_anima/.

BARRIO ANDRÉS, M., "El régimen jurídico de los delitos cometidos en Internet en el derecho español tras la reforma penal de 2010", en en VVAA, *Delincuencia informática. Tiempos de cautela y amparo*, ed. Aranzadi, primera edición, Navarra, 2012.

BELING, E. V., *Esquema de Derecho Penal. La doctrina del delito – tipo*, ed. Librería "El Foro", Buenos Aires, 2002, traducido por SOLER, S.

BOIX REIG, J., "Consideraciones sobre la protección penal de la intimidad y del honor e informática", en *Anales de la Universidad de Alicante. Facultad de Derecho,* 1983, 2. Disponible en https://rua.ua.es/dspace/bitstream/10045/55007/1/Anales_Fac_Derecho_02_02.pdf consultado el 27 de septiembre de 2016.

BOIX REIG, J. (Dir.) y VVAA, *Derecho Penal. Parte Especial. Volumen I. La protección penal de los intereses jurídicos personales (adaptado a las reformas de 2010 del Código penal)*, ed. Iustel, primera edición, Madrid, 2010.

BOIX REIG, J. (Dir.) y JAREÑO LEAL, A. (Coord.), *La protección jurídica de la intimidad*, ed. Iustel, primera edición, Madrid, 2010.

BOLEA BORDÓN, C. en CORCOY BIDASOLO, M. y MIR PUIG, S. (Dir.) y VVAA, *Comentarios al Código Penal. Reforma LO 5/2010*, ed. Tirant lo Blanch, Valencia, 2011.

BORJA JIMÉNEZ, E., *Curso de política criminal*, ed. Tirant lo Blanch, segunda edición, Valencia, 2011.

BUNYAN, T., "Trevi, Europol and the European state", en *Statewatching the new Europe*, 1993, consultado el 14 de septiembre de 2016 en http://www.statewatch.org/news/handbook-

trevi.pdf.

CAMACHO VIZCAÍNO, A. y CORTÉS LABADÍA, J. P., " Partidos políticos y responsabilidad penal de las personas jurídicas", *Diario La Ley on-line*, nº 8586, de 20 de julio de 2015, ed. La Ley, Madrid.

CARBONELL MATEU, J.C., "Reflexiones sobre el abuso del Derecho penal y la banalización de la legalidad", en ARROYO ZAPATERO, L. A. y BERDUGO GÓMEZ DE LA TORRE, I. (Coords.), *Homenaje al Dr. Marino Barbero Santos: "in memoriam"*, ed. Universidad de Castilla-La Mancha, Cuenca, 2001.

CARBONELL MATEU, J. C., y GONZÁLEZ CUSSAC, J. L., "Artículo 167", en VIVES ANTÓN, T. (Coord.) y VVAA, *Comentarios al Código Penal de 1995*, ed. Tirant Lo Blanch, Valencia, 1996.

CARBONELL MATEU, J. C., y GONZÁLEZ CUSSAC, J. L., "Artículo 198", en VIVES ANTÓN, T. (Coord.) y VVAA, *Comentarios al Código Penal de 1995*, ed. Tirant Lo Blanch, Valencia, 1996.

CARBONELL MATEU, J. C., y GONZÁLEZ CUSSAC, J. L., "Delitos contra la Intimidad, el Derecho a la Propia Imagen y la Inviolabilidad del Domicilio", en VVAA, *Derecho Penal. Parte especial*, ed. Tirant Lo Blanch, Valencia, 2010.

CARRARA, F., *Programa de Derecho Criminal. Parte general.*

*Volumen I*, ed. Temis, Bogotá, 1988, traducido por ORTEGA TORRES, J. J., y GUERRERO, J.

CARRASCO ANDRINO, M. M., "El Delito de Acceso Ilícito a los Sistemas Informáticos", en ÁLVAREZ GARCÍA, F. J., GONZÁLEZ CUSSAC, J. L. (Dir.) y VVAA, *Comentarios a la Reforma Penal de 2010*, ed. Tirant Lo Blanch, Valencia, 2010.

CASTELLÓ NICÁS, N., "Delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio, y delitos contra el honor", en MORILLAS CUEVA, L. (Dir.) y VVAA, *Estudios sobre el Código penal reformado*, ed. Dykinson, Madrid, 2015.

CASTELLS, M., *La era de la información. Economía, sociedad y cultura. Volumen II: El poder de la identidad*, Alianza Editorial, Madrid, 1998.

CASTILLO JIMENEZ, C., *Protección del derecho a la intimidad y uso de las nuevas tecnologías de la información*, Universidad de Huelva, Huelva, 2001, consultado el 28 de marzo de 2012 en http://www.uhu.es/derechoyconocimiento/DyC01/A02.pdf.

CASTRO, F., "Mentiras deliberadas, muertes extrañas y agresión a la economía mundial", en *Diario Granma*, 18 de septiembre de 2007, consultado el 14 de septiembre de 2016 en http://www.granma.cu/granmad/secciones/reflexiones/esp-049.html.

CEREZO MIR, J., *Derecho Penal. Parte General-lecciones*, ed. UNED, Madrid, 2000.

CLIFF, A., "Intrusion detection systems terminology", en *Symantec.com*, 3 de julio de 2001, consultado el 14 de septiembre de 2016 en http://www.symantec.com/connect/articles/intrusion-detection-systems-terminology-part-one-h.

CLIMENT DURÁN, C., "Título XXI. Delitos contra la Constitución. Capítulo V. De los delitos cometidos por los funcionarios públicos contra las garantías constitucionales. Sección 1ª. De los delitos cometidos por los funcionarios públicos contra la libertad individual", en GÓMEZ TOMILLO, M. (Dir.) y VVAA, *Comentarios al Código Penal*, ed. Lex Nova, primera edición, Valladolid, 2010.

COBO DEL ROSAL, M., *Comentarios al Código Penal, Tomo VII*, ed. Derecho Reunidas, Madrid, 2003.

COLÁS TURÉGANO, A., "Nuevas conductas delictivas contra la intimidad (arts. 197, 197 bis, 197 ter)", en GONZÁLEZ CUSSAC, J.L. (Dir.) y VVAA, *Comentarios a la reforma del Código penal de 2015*, ed. Tirant lo Blanch, Valencia, 2015.

COLÁS TURÉGANO, A., "El delito de instrusismo informático tras la reforma del CP español de 2015", en *Revista Boliviana de Derecho*, nº 21, enero 2016, disponible en http://www.scielo.org.bo/pdf/rbd/n21/n21_a10.pdf, consultado el 18 de septiembre de 2016.

COTS MARFIL, A., "Una aproximación al artículo 197.2 del Código Penal Vigente", en *Actualidad Jurídica Aranzadi,* nº

757/2008, Pamplona, 2008.

CRADDOCK, A., "Spamming Lawyer Disbarred", en *wired.com*, 7 de octubre de 1997, consultado el 14 de septiembre de 2016 en http://archive.wired.com/politics/law/news/1997/07/5060.

CREMADES, J., FERNÁNDEZ-ORDÓÑEZ, M.A. e ILLESCAS, R. (Coords.), *Régimen jurídico de Internet*, ed. La Ley, Madrid, 2002.

CUERDA ARNAU, M. L., "Delitos contra el orden público", en GONZÁLEZ CUSSAC, J. L. (Coord.), y VVAA *Derecho penal. Parte especial*, ed. Tirant Lo Blanch, Valencia, 2016.

DE LA CUESTA ARZAMENDI, J. L., PÉREZ MACHÍO, A. I. y SAN JUAN GUILLÉN, C., "*Aproximaciones Criminológicas a la Realidad de los Ciberdelitos"*, en DE LA CUESTA ARZAMENDI, J. L. (Dir.), y VVAA, *Derecho Penal Informático*, ed. Civitas, Pamplona, 2010.

DE LA CUESTA ARZAMENDI, J. L. (Dir.) y VVAA, *Derecho Penal Informático*, Ed. Civitas, Pamplona, 2010.

DE LA CUESTA ARZAMENDI, J. L., "Responsabilidad penal de las personas jurídicas en el Derecho español", *Revista Peruana de Ciencias Penales*, nº 26, 2013.

DE LA MATA BARRANCO, N. J., "Los delitos vinculados a las tecnologías de la información y comunicación en el Código Penal: panorámica general", en *Cuadernos penales José María Lidón, nº*

*4. Delito e informática: algunos aspectos,* Universidad de Deusto, Bilbao, 2007.

DE LA MATA BARRANCO, N. J., *Derecho penal europeo y legislación española: las reformas del Código penal*. Ed. Tirant lo Blanch, Valencia, 2015.

DE LA MATA BARRANCO, N. J. y HERNÁNDEZ DÍAZ, L., "Un ejemplo de delitos informáticos: delitos contra sistemas y datos en el Código penal español, ¿delitos de daños?", en DE LA CUESTA ARZAMENDI, J. L. (Dir.) y VVAA, *Derecho Penal Informático,* Ed. Civitas, Pamplona, 2010.

DE LA MATA BARRANCO, N. J. y HERNÁNDEZ DÍAZ, L., "Los delitos vinculados a la informática en el Derecho penal español", en DE LA CUESTA ARZAMENDI, J. L. (Dir.) y VVAA *Derecho Penal Informático,* Ed. Civitas, Pamplona, 2010.

DE URBANO CASTRILLO, E., "Los delitos informáticos tras la reforma del CP de 2010", en en VVAA, *Delincuencia informática. Tiempos de cautela y amparo,* ed. Aranzadi, primera edición, Navarra, 2012.

DE VICENTE MARTÍNEZ, R., *Vademécum de Derecho Penal*, 3º edición, ed. Tirant Lo Blanch, Valencia, 2014.

DEL MORAL GARCÍA, A., SERRANO BUTRAGUEÑO, I. (Coords.) y VVAA, *Código Penal, Comentarios y Jurisprudencia, Tomo II*, ed. Comares, tercera edición, Granada, 2001.

DEL ROSAL BLASCO, B., "Responsabilidad penal de personas jurídicas: títulos de imputación y requisitos para la exención", en MORILLAS CUEVA, L. (Dir.) y VVAA, *Estudios sobre el Código penal reformado*, ed. Dykinson, Madrid, 2015.

DELIO, M., "Battered computers – an epidemic", en *Wired News*, 6 de mayo 2001, consultado el 14 de septiembre de 2016 en hhttp://archive.wired.com/culture/lifestyle/news/2001/06/44284?currentPage=all.

DÍAZ MARTÍNEZ, M., "El factor criminógeno de las TIC", en PÉREZ GIL, J. y VVAA, *El proceso penal en la sociedad de la información*, ed. La Ley, Madrid, 2012.

DÍAZ Y GARCÍA CONLLEDO, M., *La autoría en Derecho penal*, ed. PPU, Barcelona, 1991.

DÍEZ RIPOLLES, J. L. y ROMEO CASABONA, C. M. (Coord.) y VVAA, *Comentarios al Código Penal, Parte Especial II*, ed. Tirant lo Blanch, Valencia, 2004.

DOPICO GÓMEZ-ALLER, J., "Responsabilidad de personas jurídicas", en ORTIZ DE URBINA GIMENO, Í. (Coord.) y VVAA, *Memento experto. Reforma penal 2010. Ley Orgánica 5/2010*, ed. Francis Lefebvre, Madrid, 2010.

DOVAL PAIS, A., *Delitos de Fraude Alimentario*, ed. Aranzadi, Navarra, 1996.

DUCKLIN P., "Anti-virus is no good" – discuss", en

*nakedsecurity*, http://nakedsecurity.sophos.com/anti-virus-is-no-good-discuss/, consultado el 14 de septiembre de 2016.

FERNÁNDEZ TERUELO, J. G., *Derecho Penal e Internet. Especial consideración de los delitos que afectan a jóvenes y adolescentes*, ed. Lex Nova, Valladolid, primera edición, 2011.

FILIOL, E., *Computer viruses: from theory to applications*, ed. Springer, Rennes, 2005

FLORES PRADAS, I., *Criminalidad informática (Aspectos sustantivos y procesales)*, ed. Tirant Lo Blanch, primera edición, Valencia, 2012.

FRÍAS MARTÍNEZ, E., "Delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio", en ROMA VALDÉS, A. (Dir.) y VVAA *Código penal comentado*, ed. Bosch, primera edición, Barcelona, 2015.

FRÍGOLS I BRINES, E., "La protección constitucional de los datos de las comunicaciones*"*, en BOIX REIG, J. (Dir.) y JAREÑO LEAL, A. (Coord.), *La protección jurídica de la intimidad*, ed. Iustel, Madrid, 2010.

GARCÍA ALBERO, R., "Delitos contra el orden público", en QUINTERO OLIVARES (Dir.) y VVAA, *Comentarios a la parte especial del Derecho penal*, ed. Aranzadi, Navarra, 2016.

GARCÍA MEXÍA, P. (Dir.), y VVAA, *Principios de Derecho de Internet*, ed. Tirant Lo Blanch, Valencia, 2005.

GERCKE, M., “Comprensión del Ciberdelito. Fenómenos, dificultades y respuesta jurídica”, en *International Telecommunication Union,* septiembre 2012, disponible en http://www.itu.int/en/ITU-D/Cybersecurity/Documents/CybcrimeS.pdf, consultado el 14 de septiembre de 2016.

GIMBERNAT ORDEIG, E., “Prólogo”, en MANZANARES SAMANIEGO, J. L., *La reforma del Código penal de 2015 conforme a las Leyes Orgánicas 1 y 2/2015, de 30 de marzo*, ed. La Ley, Madrid, 2015.

GÓMEZ-JARA DÍEZ, C., "Delito corporativo y responsabilidad penal de las personas jurídicas: un desarrollo coherente de la jurisprudencia del Tribunal Supremo", *Diario La Ley on-line*, nº 8830, de 23 de septiembre de 2016, ed. La Ley, Madrid.

GÓMEZ NAVAJAS, J., *La protección de datos personales. Un análisis desde la perspectiva del Derecho Penal*. Editorial Aranzadi, Navarra, 2005.

GÓMEZ RIVERO, M. C. (Coord.) y VVAA, *Nociones Fundamentales de Derecho Penal*, ed. Tecnos. Madrid, 2010.

GÓMEZ TOMILLO, Manuel (Dir.) y VVAA, *Comentarios al Código Penal*, ed. Lex Nova, primera edición, Valladolid, 2010.

GONZÁLEZ CUSSAC, J. L., "Estrategias legales frente a las ciberamenazas", en *Cuadernos de estrategia (Ministerio de Defensa),* ed. Ministerio de Defensa: Instituto Español de Estudios

Estratégicos, nº 149, Madrid, 2011.

GONZÁLEZ CUSSAC, J. L. (Dir.) y VVAA, *Comentarios a la reforma del Código penal de 2015*, ed. Tirant lo Blanch, Valencia, 2015.

GONZÁLEZ CUSSAC, J. L., "Delitos contra la libertad", en GONZÁLEZ CUSSAC, J. L. (Coord.), y VVAA, *Derecho penal. Parte especial*, ed. Tirant Lo Blanch, Valencia, 2016.

GONZÁLEZ CUSSAC, J. L., "Delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio", en GONZÁLEZ CUSSAC, J. L. (Coord.), y VVAA, *Derecho penal. Parte especial*, ed. Tirant Lo Blanch, Valencia, 2016.

GONZÁLEZ CUSSAC, J. L. (Coord.), y VVAA, *Derecho penal. Parte especial*, ed. Tirant Lo Blanch, Valencia, 2016.

GONZÁLEZ RUS, J. J., "La criminalidad organizada en el Código Penal Español. Propuestas de reforma", en *Anales de derecho*, nº 30, ed. Universidad de Murcia, Murcia, 2012, disponible en http://revistas.um.es/analesderecho/article/view/161841/142081, consultado el 9 de abril de 2017.

GÓRRIZ ROYO, ELENA Mª, *El concepto de autor en el Derecho penal*, ed. Tirant Lo Blanch, Valencia, 2008.

GUARDIOLA GARCÍA, J., "Corrección de errores en el BOE y principio de legalidad en materia penal", *La Ley Penal, nº 10, Sección Legislación aplicada a la práctica*, ed. La Ley, noviembre

2004.

GUTIÉRREZ FERNÁNDEZ, B., *Examen histórico del Derecho penal*, ed. Analecta, Pamplona, 2003.

HERNÁNDEZ DÍAZ, L., "*Aproximación a un Concepto de Derecho Penal Informático"*, en DE LA CUESTA ARZAMENDI, J. L. (Dir.), y VVAA, *Derecho Penal Informático*. ed. Civitas, Pamplona, 2010.

HUBBELL NYCUM, S., "Legal problems of computer abuse", en *Washington University Law Reviex*, 1977, consultado el 14 de septiembre de 2016 en http://openscholarship.wustl.edu/cgi/viewcontent.cgi?article=2611&context=law_lawreview.

HURTADO ADRIÁN, A., "Accesos informáticos ilícitos (art. 197 apdo. 3)", en JUANES PECES, A. (Dir.) y VVAA, *Reforma del Código penal. Perspectiva económica tras la entrada en vigor de la Ley Orgánica 5/2010 de 22 de junio. Situación jurídico-penal del empresario*, ed. El Derecho, Madrid, 2010.

JAREÑO LEAL, A., "Delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio (2). Allanamiento de morada ", en BOIX REIG, J. (Dir.) y VVAA, *Derecho Penal. Parte Especial. Volumen I. La protección penal de los intereses jurídicos personales*, ed. Iustel, segunda edición, Madrid, 2016.

JORGE BARREIRO, A., actualizado por GUÉREZ TRICARICO, P. "Delitos contra la intimidad, el derecho a la propia imagen y la

inviolabilidad del domicilio", en MOLINA FERNÁNDEZ, F. (Coord.) y VVAA, *Memento práctico penal 2016*, ed. Francis Lefebvre, Madrid, 2015.

JORGE BARREIRO, A., actualizado por GUÉREZ TRICARICO, P., "Delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio", en MOLINA FERNÁNDEZ, F. (Coord.) y VVAA, *Memento práctico penal 2017*, ed. Francis Lefebvre, Madrid, 2016.

JUANATEY DORADO, C. y DOVAL PAIS, A., "Límites de la protección penal de la intimidad frente a la grabación de conversaciones o imágenes", en BOIX REIG, J. (Dir.) y JAREÑO LEAL, A. (Coord.), *La protección jurídica de la intimidad*, ed. Iustel, Madrid, 2010.

JUANES PECES, A. (Dir.) y VVAA, *Reforma del Código penal. Perspectiva económica tras la entrada en vigor de la Ley Orgánica 5/2010 de 22 de junio. Situación jurídico-penal del empresario*, ed. El Derecho, Madrid, 2010.

JUANES PECES, A., "Introducción a la responsabilidad penal de las personas jurídicas. Consideraciones generales y problemas sustantivos y procesales que dicha responsabilidad suscita", en JUANES PECES, A. (Dir.) y VVAA, *Memento Experto. Responsabilidad penal y procesal de las personas jurídicas*, ed. Francis Lefebvre, Madrid, 2015.

KABAY, M. E., "A brief History of computer crime: an

introduction for students", en *School of Graduate Studies*, 2008, consultado el 14 de septiembre de 2016 en http://www.mekabay.com/overviews/history.pdf.

LAURENZO COPELLO, P., *El resultado en Derecho Penal*, ed. Tirant Lo Blanch Alternativa, Valencia, 1992.

LEVY, S., *Hacker*, ed. O'Reilly, Sebastopol (California), mayo de 2010.

LÍBANO MANZUR, C., "Los Delitos de Hacking en sus Diversas Manifestaciones", en *REDI Revista Electrónica de Derecho Informático*, nº 21, abril 2000.

LLORIA GARCÍA, P., *El delito de intrusismo profesional (bien jurídico y configuración del injusto)*, ed. Tirant lo Blanch, Valencia, 2001.

LLORIA GARCÍA, P., *Aproximación al estudio del delito permanente*, ed. Comares, Granada, 2006.

LLORIA GARCÍA, P., "Delitos y redes sociales: los nuevos atentados a la intimidad, el honor y la integridad moral. Especial referencia al sexting", *La Ley Penal*, nº 105, ed. Wolters Kluwer, noviembre-diciembre 2013.

LLORIA GARCÍA, P., "Menores, redes sociales e intimidad: consentimiento y tutela. Algunas consideraciones", en ANARTE BORRALO, E., MORENO MORENO, F. y GARCÍA RÚIZ, C. (Coordinadores), *Nuevos conflictos sociales. El papel de la*

*privacidad*, ed. Iustel, Madrid, 2015.

LÓPEZ ZAMORA, P., *El ciberespacio y su ordenación*, ed. Difusión Jurídica y Temas de Actualidad, Madrid, 2006.

LUZÓN CUESTA, J. M., *Compendio de Derecho Penal. Parte General*. Ed. Dykinson, Madrid, 2000.

LUZÓN CUESTA, J. M., *Compendio de Derecho penal. Parte especial*. Ed. Dykinson, Madrid, 2000.

LUZÓN CUESTA, J. M., *Compendio de Derecho Penal. Parte General*. Ed. Dykinson, Madrid, 2016.

LUZÓN PEÑA, D. M., *Lecciones de Derecho penal. Parte General*, ed. Tirant lo Blanch, segunda edición, Valencia, 2012.

LUZÓN PEÑA, D. M., *Lecciones de Derecho penal. Parte General*, ed. Tirant lo Blanch, tercera edición, Valencia, 2016.

MANZANARES SAMANIEGO, J. L., *La reforma del Código penal de 2015 conforme a las Leyes Orgánicas 1 y 2/2015, de 30 de marzo*, ed. La Ley, Madrid, 2015.

MARCHENA GÓMEZ, M., "Delitos contra la Intimidad", en DEL MORAL GARCÍA, A., SERRANO BUTRAGUEÑO, I. (Coords.) y VVAA, *Código Penal: Comentarios y Jurisprudencia*, *Tomo II*, ed. Comares de Ciencia Jurídica, Granada, 2001.

MATA Y MARTÍN, R. M., "La protección penal de datos como tutela de la intimidad de las personas. Intimidad y nuevas tecnologías ", en *Revista penal*, nº 18, 2006, consultado el 28 de

marzo de 2012 en http://www.uhu.es/revistapenal/index.php/penal/article/viewFile/291/282.

MAYER, M. E., *Derecho Penal. Parte General*, ed. B de f, Buenos Aires, 2007, traducido por POLITOFFF LIFSCHITZ, S.

MÉNDEZ RODRÍGUEZ, C., "Delitos de peligro y bienes jurídicos colectivos", en *Nuevo Foro Penal*, nº 44, junio, 1989.

MÉNDEZ RODRÍGUEZ, C., *Los delitos de peligro y sus técnicas de tipificación*, ed. Universidad Complutense de Madrid, Madrid, 1993.

MENÉNDEZ MATO, J. C. y GAYO SANTA CECILIA, M. A., *Derecho e informática: ética y legislación*, ed. Bosch, Barcelona, 2014.

MEZGER, E., *Tratado de Derecho penal*, Tomo I, ed. Revista de Derecho privado, segunda edición, Madrid, 1935, traducido por RODRÍGUEZ MUÑOZ, J.A.

MEZGER, E., *Tratado de Derecho penal*, Tomo II, ed. Revista de Derecho privado, segunda edición, Madrid, 1935, traducido por RODRÍGUEZ MUÑOZ, J.A.

MILLER, A. R., "The national data center and personal privacy", en *The Atlantic*, noviembre de 1967, consultado el 14 de septiembre de 2016 en http://blog.modernmechanix.com/the-national-data-center-and-personal-privacy/.

MIR PUIG, S. (Comp.) y VVAA, *Delincuencia informática*, ed. Promociones y Publicaciones Universitarias, Barcelona, 1992.

MIR PUIG, S., *Derecho penal. Parte general*, ed. Reppertor, novena edición, Barcelona, 2011.

MIR PUIG, S., *Derecho penal. Parte general*, ed. Reppertor, décima edición, Barcelona, 2016.

MIRÓ LLINARES, F., "Los Delitos Informáticos*"*, en ORTIZ DE URBINA GIMENO, Í. (Coord.) y VVAA, *Memento experto. Reforma penal 2010. Ley Orgánica 5/2010*, ed. Francis Lefebvre, Madrid, 2010.

MIRÓ LLINARES, F., *El cibercrimen. Fenomenología y criminología de la delincuencia en el ciberespacio*, ed. Marcial Pons, primera edición, Madrid, 2012.

MOLINA FERNÁNDEZ, F. (Coord.) y VVAA, *Memento práctico penal 2016*, ed. Francis Lefebvre, Madrid, 2015.

MOLINA FERNÁNDEZ, F. (Coord.) y VVAA, *Memento práctico penal 2017*, ed. Francis Lefebvre, Madrid, 2016.

MOLINA FERNÁNDEZ, F., "Autoría y participación delictiva", en MOLINA FERNÁNDEZ, F. (Coord.) y VVAA, *Memento práctico penal 2017*, ed. Francis Lefebvre, Madrid, 2016.

MORALES GARCÍA, O., "Delincuencia informática: instrusismo, sabotaje informático y uso ilícito de tarjetas", en QUINTERO OLIVARES, G. (Dir.) y VVAA, *La reforma penal de 2010:*

*Análisis y comentarios*, ed. Thomson reuters, Navarra, 2010.

MORALES GARCÍA, O., "Comentario a los delitos informáticos de los arts. 197, 248 y 264 CP", en VVAA, *Delincuencia informática. Tiempos de cautela y amparo*, ed. Aranzadi, primera edición, Navarra, 2012.

MORALES PRATS, F., *La tutela penal de la intimidad: privacy e informática*, ed. Destino, Barcelona, 1984.

MORALES PRATS, F., "Título X. Delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio", en QUINTERO OLIVARES, G. (Dir.), MORALES PRATS, G. (Coord.), *Comentarios a la Parte especial del Derecho penal*, ed. Aranzadi, novena ed., Navarra, 2011.

MORALES PRATS, F., "La reforma de los delitos contra la intimidad artículo 197 CP", en QUINTERO OLIVARES, G. (Dir.), y VVAA, *Comentario a la reforma penal de 2015*, ed. Aranzadi, Navarra, 2015.

MORALES PRATS, F., "Delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio", en QUINTERO OLIVARES (Dir.) y VVAA, *Comentarios a la parte especial del Derecho penal*, ed. Aranzadi, Navarra, 2016.

MORENO ALCÁZAR, M. A., *El concepto penal de incendio desde la teoría del caos (una perspectiva sistemática de los bienes jurídicos colectivos, del peligro y de su causalidad)*, ed. Tirant Lo Blanch, Valencia, 2002.

MORÓN LERMA, E., *Internet y Derecho penal: <<Hacking>> y otras conductas ilícitas en la red*, ed. Aranzadi, segunda edición, Navarra, 2002.

MORILLAS CUEVA, L., "La cuestión de la responsabilidad penal de las personas jurídicas", *Anales de Derecho*, nº 29, 2011.

MORILLAS CUEVA (Dir.) y VVAA, *Estudios sobre el Código penal reformado*, ed. Dykinson, Madrid, 2015.

MOYNA MÉNGUEZ, J., en VVAA, *Código Penal*, ed. Colex, 13ª edición, Madrid, 2010.

MUÑOZ CONDE, F., *Derecho penal. Parte especial*, ed. Tirant Lo Blanch, Valencia, 2010.

MUÑOZ CONDE, F., *Derecho penal. Parte especial*, ed. Tirant lo Blanch, Valencia, 2015.

MUÑOZ CONDE, F. y GARCÍA ARÁN, M., *Derecho Penal. Parte General*, ed. Tirant lo Blanch, 9ª edición, Valencia, 2015.

MUÑOZ CUESTA, J. y RUIZ DE ERENCHUN ARTECHE, E., *Cuestiones prácticas sobre la reforma penal de 2015*, ed. Aranzadi, primera edición, Navarra, 2015.

MUÑOZ MACHADO, S. (Dir.) y VVAA, *Diccionario del español jurídico*, ed. Espasa, primera edición, Barcelona, 2016.

NIETO MARTÍN, A., *La responsabilidad penal de las personas jurídicas: un modelo legislativo*, ed. Iustel, Madrid, 2008.

NIETO MARTÍN, A. y GARCÍA MORENO, B., "Derecho penal

europeo y comparado. Cooperación judicial", en JUANES PECES, A. (Dir.) y VVAA, *Memento Experto. Responsabilidad penal y procesal de las personas jurídicas*, ed. Francis Lefebvre, Madrid, 2015.

NUÑEZ CASTAÑO, E., "Lección XII. Delitos contra la intimidad el derecho a la propia imagen y la inviolabilidad del domicilio", en GÓMEZ RIVERO, M. C. (Coord.) y VVAA, *Nociones Fundamentales de Derecho Penal*, ed. Tecnos. Madrid, 2010.

ORTIZ DE URBINA GIMENO, Í. (Coord.) y VVAA, *Memento experto. Reforma penal 2010. Ley Orgánica 5/2010,* ed. Francis Lefebvre, Madrid, 2010.

ORTIZ PRADILLO, J. C., "<<Hacking>> legal al servicio de la investigación criminal: nuevos instrumentos para la investigación y prueba de la delincuencia informática", en VVAA, en VVAA, *Delincuencia informática. Tiempos de cautela y amparo*, ed. Aranzadi, primera edición, Navarra, 2012.

ORTS BERENGUER, E. y ROIG TORRES, M., *Delitos informáticos y delitos comunes cometidos a través de la informática*, ed. Tirant Lo Blanch, Valencia, 2001.

ORTS BERENGUER, E. y GONZÁLEZ CUSSAC, J. L., Compendio de Derecho penal, parte general, ed. Tirant Lo Blanch, Valencia, 2016.

PATTARO, E. (Dir.), *Manuale di diritto dell'informatica e delle nuove tecnologie*, ed. Clueb, Bolonia, 2000.

PECORELLA, C., “El acceso abusivo a los sistemas informáticos o telemáticos”, en ANARTE BORRALO, E., MORENO MORENO, F. y GARCÍA RÚIZ, C. (Coordinadores), *Nuevos conflictos sociales. El papel de la privacidad*, ed. Iustel, Madrid, 2015.

PICOTTI, L., “National legislation implementing the Convention on Cybercrime – Comparative analysis and good practices”, en *Council of Europe*, 24 de agosto de 2008, consultado el 29 de octubre de 2015 en https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802fa3bc.

PORRES ORTIZ DE URBINA, E., "Responsabilidad penal de las personas jurídicas", *Revista de Jurisprudencia El Derecho*, nº 2, ed. El Derecho, 1 de junio de 2015.

POZUELO PÉREZ, L., “Circunstancias agravantes y mixta de parentesco”, en MOLINA FERNÁNDEZ, F. (Coord.) y VVAA, *Memento práctico penal 2017*, ed. Francis Lefebvre, Madrid, 2016.

QUERALT JIMÉNEZ, J. J., *Derecho penal español. Parte especial*, ed. Atelier, sexta edición, Barcelona, 2010.

QUERALT JIMÉNEZ, J. J., *Derecho penal español. Parte especial*, ed. Tirant lo Blanch, primera edición, Valencia, 2015.

QUINTERO OLIVARES, G., “La autotutela, los límites al poder sancionador de la Administración Pública y los principios inspiradores del Derecho Penal”, en *Revista de administración pública*, nº 126, 1991, disponible en

https://dialnet.unirioja.es/descarga/articulo/17106.pdf, consultado el 4 de enero de 2017.

QUINTERO OLIVARES, G. (Dir.) y VVAA, *Comentarios a la parte especial del Derecho penal*, ed. Aranzadi, séptima edición, Navarra, 2008.

QUINTERO OLIVARES, G., con la colaboración de MORALES PRATS, F., *Parte general del Derecho penal*, ed. Aranzadi, Navarra, 2010, p. 648.

QUINTERO OLIVARES, G. (Dir.) y VVAA, *La reforma penal de 2010: Análisis y comentarios*, ed. Aranzadi, Navarra, 2010.

QUINTERO OLIVARES, G. (Dir.), MORALES PRATS, G. (Coord.), *Comentarios a la parte especial del Derecho penal*, ed. Aranzadi, novena ed., Navarra, 2011.

QUINTERO OLIVARES, G., *La reforma del Código penal y los problemas alrededor de su entrada en vigor*, en *Revistaiuris*, Septiembre, nº 152, consultado el 28 de marzo de 2012 en http://www.revistaiuris.com/ver_pdf.asp?idArt=64014.

QUINTERO OLIVARES, G., "La responsabilidad penal de los Partidos como personas jurídicas", *Actualidad Jurídica Aranzadi*, nº 859/2013.

QUINTERO OLIVARES, G. (Dir.), y VVAA, *Comentario a la reforma penal de 2015*, ed. Aranzadi, Navarra, 2015.

QUINTERO OLIVARES (Dir.) y VVAA, *Comentarios a la parte*

*especial del Derecho penal*, ed. Aranzadi, Navarra, 2016.

QUINTERO OLIVARES, G., *Pequeña historia penal de España*, ed. Iustel, Madrid, 2017.

RAGUÉS I VALLÉS, 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.), PASTOR MUÑOZ, N. (Coord.) y VVAA, *El nuevo Código Penal. Comentarios a la reforma*, ed. La Ley, Navarra, 2011.

RAYMOND, E. S., "A brief History of Hackerdom", en *Eric's random writings*, consultado el 14 de septiembre de 2016 en http://catb.org/esr/writings/hacker-history/hacker-history.html#toc3.

RIQUERT, M. A., "Protección contra la delincuencia informática en el MERCOSUR", en http://riquertdelincuenciainformatica.blogspot.com/2007/11/proteccin-contra-la-delincuencia.html, Universidad Nacional de Mar del Plata, 11 de noviembre de 2007.

RIVAS VERDES-MONTENEGRO, C., "La responsabilidad penal de las personas jurídicas: problemas dogmáticos y soluciones legislativas", *La Ley Penal*, nº 75, ed. La Ley, Madrid, 2010.

RODRÍGUEZ MONTAÑÉS, T., *Delitos de peligro, dolo, e imprudencia*, ed. Universidad Complutense de Madrid, Madrid, 1994.

RODRÍGUEZ MOURULLO, G. (Dir.) y VVAA, *Comentarios al Código penal*, ed. Civitas, Madrid, 1997.

RODRIGUEZ MOURULLO, G., ALONSO GALLO, J., LASCURAÍN SÁNCHEZ, J.A., "Derecho penal e Internet", en CREMADES, J., FERNÁNDEZ-ORDÓÑEZ, M.A., ILLESCAS, R. (Coords.), *Régimen jurídico de Internet*, ed. La Ley, Madrid, 2002.

RODRÍGUEZ RAMOS, L., *Compendio de Derecho Penal. Parte General*, ed. Dykinson, 2ª edición, Madrid, 2010.

RODRÍGUEZ RAMOS, L. (Dir.) y VVAA, *Código Penal. Concordado y comentado con jurisprudencia y leyes penales especiales y complementarias*, ed. La Ley, quinta edición, Madrid, 2015.

ROMA VALDÉS, A., "El delito de organizaciones y grupos criminales", en *Estudios jurídicos*, nº 2012, ed. Ministerio de Justicia, Centro de Estudios Jurídicos, Madrid, 2012, p. 15, disponible en http://www.academia.edu/2394755/EL_DELITO_DE_ORGANIZACIONES_Y_GRUPOS_CRIMINALES, consultado el 9 de abril de 2017.

ROMA VALDÉS, A. (Dir.) y VVAA, *Código penal comentado*, ed. Bosch, primera edición, Barcelona, 2015.

ROMEO CASABONA, C. M., *Los delitos de descubrimiento y revelación de secretos. Especial consideración a su comisión en*

*conexión con las nuevas tecnologías de la información y de la comunicación*, ed. Tirant Lo Blanch, Valencia, 2005.

ROMEO CASABONA, C. M., "Derecho Penal y libertades de expresión y comunicación en Internet", en ARMAZA ARMAZA, Emilio José (Coord.), y VVAA, *La Adaptación del Derecho Penal al Desarrollo Social y Tecnológico*, ed. Comares, Granada, 2010.

ROMEO CASABONA, C. M. (Dir.) y VVAA, *El cibercrimen nuevos retos jurídico-penales, nuevas respuestas político-criminales*, ed. Comares, Granada, 2006.

RUEDA MARTÍN, M. Á., "Los ataques contra los sistemas informáticos: conductas de hacking. Cuestiones político-criminales", en ARMAZA ARMAZA, Emilio José (Coord.), y VVAA, *La Adaptación del Derecho Penal al Desarrollo Social y Tecnológico*, ed. Comares, Granada, 2010.

RUEDA MARTÍN, M. A., "La relevancia penal del consentimiento del menor de edad en relación con los delitos contra la intimidad y la propia imagen (especial consideración a la disponibilidad de la propia imagen del menor de edad en el ciberespacio)", en *Indret*, Barcelona, octubre de 2013, disponible en http://www.raco.cat/index.php/InDret/article/view/270185/357761, consultado el 15 de octubre de 2016.

SALAS, I., GONZÁLEZ R. y RIVEROS O., "Formulación de proyectos sustentables de acceso universal mediante el uso de las TICs", en *Boletín Electrónico infoCITEL*, nº 16 – Octubre, 2005,

consultado el 28 de marzo de 2012 en http://www.oas.org/en/citel/infocitel/2005/octubre/universal-1_e.asp

SALVADORI, I., "Los nuevos delitos informáticos introducidos en el Código penal español con la Ley Orgánica 5/2010. Perspectiva de derecho comparado", en *ADPCP*, ed. Ministerio de Justicia (Centro de publicaciones) y Agencia Estatal Boletín Oficial del Estado, vol. LXIV, 2011, consultado el 10 de octubre de 2015 en https://www.boe.es/publicaciones/anuarios_derecho/abrir_pdf.php?id=ANU-P-2011-10022100252_ANUARIO_DE_DERECHO_PENAL_Y_CIENCIAS_PENALES_Los_nuevos_delitos_inform%E1ticos_introducidos_en_el_C%F3digo_Penal_espa%F1ol_con_la_Ley_Org%E1nica_5/2010._Perspectiva_de_derecho_comparado

SÁNCHEZ DOMINGO, M. B., "Delincuencia Informática y el delito de intrusismo informático: aspectos de su regulación en instrumentos normativos europeos y su transposición al Código Penal español acorde a la LO 5/2010 de reforma de Código Penal español", en *RGDP de Iustel*, nº 18, 2012, disponible en http://www.iustel.com/v2/revistas/detalle_revista.asp?id_noticia=412629, consultado el 6 de enero de 2017.

SÁNCHEZ MAGRO, A., "El ciberdelito y sus implicaciones procesales", en GARCÍA MEXÍA, P. (Dir.) y VVAA, *Principios de Derecho de Internet*, ed. Tirant Lo Blanch, Valencia, 2005.

SÉDALLIAN, V., "Accès à une base de données mal sécurisée et responsabilités pénales", en *Journaldunet*, 6 de febrero de 2003, consultado el 29 de octubre de 2015 en http://www.journaldunet.com/solutions/0302/030206_trib_juridique.shtml.

SELTZER, L., "The Morris Worm: Internet malware turns 25", en *Zero Day*, 2 de noviembre de 2013, consultado el 14 de septiembre de 2016 en http://www.zdnet.com/the-morris-worm-internet-malware-turns-25-7000022740/.

SIEBER, U., "Documentación para una aproximación al delito informático", en MIR PUIG, S. (Comp.) y VVAA, *Delincuencia informática*, ed. Promociones y Publicaciones Universitarias, Barcelona, 1992.

SIEBER, U., "Legal aspects computer-related crime – COMCRIME-Study prepared for the European Commission", *University of Würzburg*, 1 de enero de 1998, consultado el 14 de septiembre de 2016 en http://www.edc.uoc.gr/~panas/PATRA/sieber.pdf.

SILVA SÁNCHEZ, J. M. (Dir.), PASTOR MUÑOZ, N. (Coord.) y VVAA, *El nuevo Código Penal. Comentarios a la reforma*, ed. La Ley, Navarra, 2011.

STERLING, B., "The hacker crackdown: law and disorder on the electronic frontier", en *Literary Freeware*, 1992, consultado el 14 de septiembre de 2016 en http://web.mit.edu/hacker/part2.html.

SUÁREZ-MIRA RODRÍGUEZ, C. (Coord.) y VVAA, *Manual de Derecho penal. Tomo II. Parte especial*, ed. Civitas, segunda edición, Madrid, 2004.

TOMÁS-VALIENTE LANUZA, C., "Título X. Delitos contra la Intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio. Capítulo I. Del descubrimiento y revelación de secretos", en GÓMEZ TOMILLO, M. (Dir.) y VVAA, *Comentarios al Código Penal*, ed. Lex Nova, primera edición, Valladolid, 2010.

VALENTI LÓPEZ, P., "La sociedad de la información en América Latina y el Caribe: TIC's y un nuevo marco institucional", en *Revista Iberoamericana de Ciencia, Tecnología, Sociedad e Innovación,* enero-abril 2002, nº 2, consultado el 28 de marzo de 2012 en http://www.campus-oei.org/revistactsi/numero2/valenti.htm.

VALLE LÓPEZ, M. V., "Los delitos de descubrimiento y revelación de secretos en el Código Penal de 2015: artículos 197, 197 *bis*, 197 *ter*, 197 *quáter*, 197 *quinquies* y 198", en *Revista Penal*, nº 39, ed. Tirant Lo Blanch, Valencia, 2017.

VELASCO NUÑEZ, E., "Delitos informáticos realizados en actuación organizada", en *Diario La Ley,* nº 7743, de 24 de noviembre de 2011.

VIVES ANTÓN, T. (Coord.) y VVAA, *Comentarios al Código Penal de 1995*, ed. Tirant Lo Blanch, Valencia, 1996.

VIVES ANTÓN, T. S. y VVAA, *Derecho penal. Parte especial*, ed. Tirant Lo Blanch, Valencia, 2010. *CD-ROM*.

VOLGYES, M. R., "The investigation, prosecution, and prevention of computer crime: a state-of-the-art review", en *The John Marshall Journal of Information Technology & Privacy Law*, 1980, p. 386, consultado el 14 de septiembre de 2016 en http://repository.jmls.edu/cgi/viewcontent.cgi?article=1607&context=jitpl.

VON LISZT, F., *Tratado de Derecho penal*, Tomo II, ed. Reus, segunda edición, Madrid, 1927, traducido por JIMÉNEZ DE ASÚA.

WARREN, S. D. y BRANDEIS, L. D.,"The right to privacy", en Harvard Law Review, Vol. IV, 15 de diciembre de 1890, nº 5, disponible en http://groups.csail.mit.edu/mac/classes/6.805/articles/privacy/Privacy_brand_warr2.html, consultado el 15 de enero de 2017

WELZEL, H., *El nuevo sistema del Derecho penal*, ed. B de F, cuarta reimpresión, Buenos Aires, 2011, traducido por CEREZO MIR, J.

WELZEL, H., *Estudios de Derecho penal*, ed. B de F, reimpresión, Buenos Aires, 2007, traducido por EDUARDO ABOSO, G., y LOW, T.

ZICCARDI, G., "Il diritto dell'informatica", en PATTARO, E. (Dir.), *Manuale di diritto dell'informatica e delle nuove tecnologie*,

ed. Clueb, Bolonia, 2000.

ZUGALDÍA ESPINAR, J. M., "La responsabilidad criminal de los partidos políticos y los sindicatos", *Revista de derecho penal y criminología, 3.ª Época*, nº 11, enero 2014.