Universitat
de les Illes Balears

TESI DOCTORAL
2016

EL DELITO DE ACCESO ILÍCITO A UN SISTEMA INFORMÁTICO

María Isabel Montserrat Sánchez-Escribano

Universitat
de les Illes Balears

TESI DOCTORAL
2016

Programa de Doctorat de Dret

EL DELITO DE ACCESO ILÍCITO A UN SISTEMA INFORMÁTICO

María Isabel Montserrat Sánchez-Escribano

Director y tutor: Antoni Gili Pascual

Doctor/a per la Universitat de les Illes Balears

LISTA DE PUBLICACIONES
(SOLO LAS RELACIONADAS CON LA TESIS)

Montserrat Sánchez-Escribano, M. I. (2014). El objeto material en el artículo 197.3 del código penal: un condicionante de la tutela de la seguridad en España *Moderno discurso penal y nuevas tecnologías: memorias [del] III Congreso Internacional de Jóvenes Investigadores en Ciencias Penales, 17, 18 y 19 de junio de 2013* (pp. 233-254): Salamanca: Ediciones Universidad de Salamanca, 2014.

Montserrat Sánchez-Escribano, M. I. (2014). Panorama normativo supranacional del delito de acceso ilícito a un sistema informático *Investigaciones en ciencias jurídicas: desafíos actuales del derecho*: Málaga: eumed.net.

Montserrat Sánchez-Escribano, M. I. (2015). Libertad informática y protección de datos: desarrollo en la jurisprudencia del Tribunal Constitucional y tutela penal en el delito de descubrimiento y revelación de secretos. *Anuario iberoamericano de justicia constitucional*(19), 323-363.

Montserrat Sánchez-Escribano, M. I. (2015). El nuevo apartado 3 del artículo 197 del Código penal: análisis e la transposición en el ámbito español del delito de acceso ilícito a un sistema informático. *Revista Peruana de Ciencias Penales*, 295-322.

BREVE RESUMEN - CASTELLANO

La tesis que se presenta tiene por objeto el estudio del acceso ilícito a un sistema informático. Esta conducta fue introducida en el Código penal español a través de la reforma operada por la Ley Orgánica 5/2010, de 22 de junio, siendo modificada la redacción del tipo penal y su ubicación sistemática por la Ley Orgánica 1/2015, de 30 de marzo. El único motivo por el cual se procedió a su incriminación se cimienta en la necesidad de transponer dos instrumentos vinculantes de carácter supranacional: por una parte, el Convenio sobre Cibercriminalidad del Consejo de Europa, firmado en Budapest el 23 de noviembre de 2001, ratificado por España el 3 de junio del año 2010, y, por otra parte, la Decisión 2005/222/JAI Consejo de la Unión Europea, de 24 febrero 2005, posteriormente sustituida por la Directiva 2013/40/EU del Parlamento Europeo y del Consejo, de 12 de agosto de 2013, relativa a los ataques a sistemas de información. En este sentido, el presente trabajo, pionero en España, tiene como objetivo arbitrar los mecanismos necesarios para su correcta interpretación y aplicación, además de solucionar las diversas incongruencias que la descripción típica conjuga.

ACCESO IlÍCITO - INTRUSISMO INFORMÁTICO - CONVENIO SOBRE CIBERCRIMEN - DIRECTIVA 2013/40/EU - ARTÍCULO 197.1 BIS - DESCUBRIMIENTO Y REVELACIÓN DE SECRETOS

BREU RESUM - CATALÀ

La tesi que es presenta té per objecte l'estudi de l'accés il·lícit a un sistema informàtic. Aquesta conducta va ser introduïda en el Codi penal espanyol a través de la reforma operada per la Llei Orgànica 5/2010, de 22 de juny, sent modificada la redacció del tipus penal i la seva ubicació sistemàtica per la Llei Orgànica 1/2015, de 30 de març. L'únic motiu pel qual es va procedir a la seva incriminació ca ver la necessitat de incorporar els mandats dirigits a tal fi derivats de dos instruments vinculants de caràcter supranacional: d'una banda, el Conveni sobre Cibercriminalidad del Consell d'Europa, signat a Budapest el 23 de novembre de 2001, ratificat per Espanya el 3 de juny de l'any 2010, i, d'altra banda, la Decisió 2005/222/JAI Consell de la Unió Europea, de 24 febrer 2005, posteriorment substituïda per la Directiva 2013/40/EU del Parlament Europeu i del Consell, de 12 d'agost de 2013, relativa als atacs a sistemes d'informació. En aquest sentit, el present treball, pioner a Espanya, té com a objectiu arbitrar els mecanismes necessaris per a la seva correcta interpretació i aplicació, a més de solucionar les diverses incongruències que la descripció típica conjuga.

ACCÉS IL·LÍCIT - INTRUSISME INFORMÀTIC - CONVENI SOBRE CIBERCRIMEN - DIRECTIVA 2013/40/EU - ARTICLE 197.1 BIS - DESCOBRIMENT I REVELACIÓ DE SECRETS

SHORT PRESENTATION - ENGLISH

This work analyzes the crime of illegal access to computer systems. The conduct was introduced in the Spanish Criminal Code by the Organic Law 5/2010, of 22 June, and subsequently modified by the Organic Law 1/2015, of 30 of march. The only reason for what illegal access is punished under the spanish criminal law is the required harmonization in this field by the Council of Europe Convention on Cybercrime, signed in Budapest the 23 of November of 2001, and the Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA. However, their content is specifically called for in some conclusions. In this sense, the present document creates the bare minimum legal basis to interprete and apply this offense and allows the legislator to take in account and solve the different problems introduced in the legal description of the crime.

ILLEGAL ACCESS - CONVENTION ON CYBERCRIME - COMPUTER RELATED CRIME

INDICE

CAPITULO II

EL TRATAMIENTO PENAL DEL ACCESO ILÍCITO EN EL DERECHO COMPARADO

SEGUNDA PARTE

ANÁLISIS DEL ARTÍCULO 197.1 BIS

CAPITULO III

EL BIEN JURÍDICO PROTEGIDO

SECCIÓN 2ª

ANÁLISIS DEL BIEN JURÍDICO PROTEGIDO EN EL ARTÍCULO 197.1 *BIS*

SECCIÓN 2ª

LA ACCIÓN DE MANTENIMIENTO

SECCIÓN 2ª

EL OBJETO MATERIAL DEL DELITO DE ACCESO ILÍCITO EN LA REFORMA OPERADA POR LA LEY ORGÁNICA 1/2015

INTRODUCCIÓN

I. OBJETO DE LA INVESTIGACIÓN

Las nuevas tecnologías de la información y la comunicación (TIC) se han convertido desde hace varias décadas en el eje central de la denominada sociedad de la información. De entre todas ellas, Internet es la herramienta de intercambio de información y comunicación que más protagonismo ha adquirido, en la medida en que no sólo permite acceder a ésta, sino también crearla, emitirla y difundirla, poniéndola a disposición de los demás usuarios de la red[1]. Internet ha eliminado, pues, las distancias geográficas en el desarrollo de actividades transfronterizas, abriendo nuevas posibilidades de intercambio de información y bienes por medios electrónicos para consumidores y empresas[2]. Sin embargo, la inabarcable dimensión que la World Wide Web ha alcanzado, ha implicado también el surgimiento de nuevos riesgos, de entre los cuales el que causa una mayor preocupación a los Estados y a la ciudadanía en general es la utilización con fines delictivos, especialmente por grupos organizados, de información de carácter confidencial obtenida ilícitamente a través del acceso no autorizado a sistemas o programas informáticos. Este uso ilegítimo ha originado en la población un importante sentimiento de inseguridad y desconfianza hacia la red y hacia la informática, fomentado en gran medida por las especiales características de la dinámica comisiva de este tipo de conductas: el potencial anonimato del autor, la ejecución a distancia, la comisión prácticamente instantánea en el tiempo, el marcado carácter transfronterizo y, en numerosas ocasiones, el elevado número de víctimas afectadas, pues se trata de delitos masa[3].

---

[1] ROMEO CASABONA, 2006: 2.

[2] MORÓN LERMA, 2002: 2.

[3] VELASCO NÚÑEZ, 2010: 46.

Dado el elevado grado de complejidad que los hechos descritos entrañan, se ha puesto de manifiesto tanto a nivel internacional como nacional la necesidad de establecer una regulación específica en materia penal que incrimine, además de la utilización ilícita de la información obtenida, el propio acceso ilícito al sistema informático, al efecto de favorecer su utilización en un marco de seguridad jurídica. De este modo, en el seno de lo que se ha definido como Derecho penal postmoderno del riesgo o de la seguridad se están adoptando iniciativas dirigidas a crear nuevas medidas de prevención y represión de los ilícitos perpetrados contra los propios sistemas informáticos.

El presente trabajo tiene como objeto de estudio del delito más básico dentro de los ilícitos que se encuadran en el fenómeno criminológico de la delincuencia informática, es decir, el acceso a un sistema informático cometido de forma ilícita. Este comportamiento ha sido el centro de la más detallada atención internacional desde la más temprana incipiencia de este fenómeno, pues constituye una barrera de protección de multitud de bienes jurídicos como pueden ser, por ejemplo, el secreto de empresa, el secreto industrial, la propiedad intelectual, la propiedad industrial, el patrimonio, el orden socioeconómico o la intimidad de las personas, ello en la medida en que su finalidad es contribuir a que el uso de la informática, y principalmente de Internet, sea un espacio seguro en el que el ciudadano y las empresas puedan llevar a cabo su tráfico de información y comunicación sometidos al menor índice de riesgo posible. La sanción de esta conducta pretende, pues, castigar la intrusión en un sistema informático ajeno con independencia de su contenido, en la medida en que éste puede ser muy variado: desde la cartera de clientes de una empresa, hasta la obra de ingenio de una persona —la tesis misma—, como fotos privadas y personales, cuyo apoderamiento supondría graves perjuicios unas veces económicos y otros personales para el titular de los mismos. La tutela se establece, en este sentido, al continente como medio para evitar la agresión de los múltiples intereses en juego.

A) LA CRIMINALIZACIÓN DEL ACCESO ILÍCITO EN ESPAÑA

Con independencia de la extrema relevancia de esta conducta de acuerdo con lo señalado en los párrafos anteriores, el acceso ilícito a un sistema informático no fue tipificado como delito en España hasta 2010. Concretamente, fue introducido en el Código penal español a través de la reforma operada por la Ley Orgánica 5/2010, de 22 de junio, siendo modificada la redacción del tipo penal y su ubicación sistemática por la Ley Orgánica 1/2015, de 30 de marzo. La introducción en el Código penal español de un tipo dirigido a castigar este comportamiento ilícito tuvo su razón de ser en la necesidad de transponer dos instrumentos vinculantes de carácter supranacional: el Convenio sobre Cibercriminalidad del Consejo de Europa, firmado en Budapest el 23 de noviembre de 2001, ratificado por España el 3 de junio del año 2010, y la Decisión 2005/222/JAI Consejo de la Unión Europea, de 24 febrero 2005, sustituida posteriormente por la Directiva 2013/40/EU del Parlamento Europeo y del Consejo, de 12 de agosto de 2013, relativa a los ataques a sistemas de información.

Se puede señalar directamente a la necesidad de transponer dichas normas como la razón principal —incluso podría decirse que única— de la introducción en el Código penal español del delito de acceso ilícito, porque, en realidad, la tipificación de esta conducta no era vista como una necesidad perentoria en la literatura penal. De hecho, numerosos autores de la **doctrina española** se manifestaron en contra de la conveniencia de incriminar el acceso ilícito fundando su opinión en dos motivos fundamentales: por un lado, su necesidad técnica, es decir, que la conducta podía ser subsumida en tipos

penales ya existentes[4] —aunque no existía acuerdo en cuáles[5]— y

[4] Para estos autores las escasa entidad de la conducta se fundamenta en que no suele existir en los autores del acceso ilícito más que una tendencia a la superación de un mero reto intelectual de demostrar que se está capacitado para vulnerar las posibles medidas de seguridad que el titular hubiese establecido para evitar el acceso al mismo. De hecho, se señala que muchas de ellas ni siquiera presentan dañosidad objetiva alguna que pueda justificar su castigo conforme a los referidos tipos delictivos, por cuando no ponen en peligro el patrimonio del dueño del sistema informático vulnerado, ni inciden sobre ordenadores que contengan informaciones que puedan ser consideradas como datos personales o secretos de carácter personal o de empresa de los que protegen los delitos del los artículos 197 y 278. En este mismo sentido se pronunció el Informe del Parlamento europeo sobre la Propuesta de la Comisión para una Decisión Marco del Consejo sobre ataques a los sistemas de información, de 4 de octubre de 2002, que criticaba la criminalización del acceso porque no se revela una auténtica conciencia de antijuricidad por parte de los jóvenes infractores. FLORES PRADA, 2012: 68. GALÁN MUÑOZ, 2009: 93. LÓPEZ ORTEGA, 2004: 119. MATELLANES RODRÍGUEZ, 2008: 63-64. MIR PUIG, 2002: 520-521. MORÓN LERMA, 2002: 55 y ss. ORTS BERENGUER y ROIG TORRES, 2005: 92.

[5] Para estos autores la pretensión de criminalizar el acceso ilícito respondía al temor de que se produjera un vacío de impunidad en la sanción de esta conducta, pero la totalidad de los actos en las que ésta puede manifestarse son susceptibles de ser subsumidos en preceptos ya vigentes del Código penal. Concretamente, como tentativas de los delitos de descubrimiento y revelación de secretos estafa informática, daños informáticos o, incluso, entre los delitos contra la propiedad intelectual o el uso indebido de un equipo terminal de telecomunicaciones, según cuál fuera la intención que guiara al sujeto en el acceso ilícito. En este mismo sentido se pronunciaba el Informe al Anteproyecto de la Ley Orgánica de reforma del Código penal de 2006 entendía el acceso ilícito plenamente subsumible en el apartado 2 del artículo 197. En consecuencia, para este sector el acceso ilícito conforma simplemente de una actualización de las formas de comisión de determinados delitos, que se verá facilitada en muchas ocasiones dado el potencial de las nuevas tecnologías informáticas. En una posición intermedia se encontraba GONZALEZ RUS, quien, si bien se manifestaba en cierta medida abierto a la necesidad de adaptar el Derecho penal vigente a las emergentes necesidades derivadas de las nuevas tecnologías, respecto del acceso ilícito consideraba que se trataba de una conducta con una inmerecida reputación y le restaba importancia a su configuración autónoma como delito afirmando, por una parte, que el acceso constituye presupuesto y medio comisivo necesario o muy frecuente en una buena parte de los supuestos delictivos, y, por otra, que será realmente excepcional el caso en el que el intruso no esté animado de ninguna finalidad punible conforme a los tipos vigentes. GONZÁLEZ RUS, 1986a: 108-109, GONZÁLEZ RUS, 1986b: 41-51, GONZÁLEZ RUS, 1999, GONZÁLEZ RUS, 2006: 243,, 247. GUTIÉRREZ FRANCÉS, 1996: 1180. MOLINA JIMENO, 2009: 6. MORÓN LERMA, 2002: 70, 63-65, PUENTE ABA, 2004: 394, ORTS BERENGUER y ROIG TORRES, 2005: 92. También DE ALFONSO LASO, 2002/2001: 509. ROVIRA DEL CANTO, 2002: 195. RUIZ VADILLO, 1989: 55-56, 73. SOTO NAVARRO, 2003: 179-180. En un primer estudio MATELLANES RODRÍGUEZ, 2000: 141-142.

que, realmente, no protegía ningún bien jurídico[6]; por otro lado, su idoneidad políticro-criminal, ya que introducir en el Código penal español el delito de acceso ilícito contradecía las exigencias del varios de los cimientos fundamentales del Derecho penal, —especialmente el principio de intervención mínima, debido a la escasa entidad que supondría sancionar el acceso ilícito de forma separada a tales comportamientos[7]—, y, también, la idea de prevención general[8].

---

[6] CORCOY BIDASOLO y PUENTE ABA niegan que pueda hablarse del surgimiento de un nuevo bien jurídico digno de protección, considerando al respecto que no se verifica esta situación base que lo fundamenta y aun menos se justificada la creación de un tipo que respondería al adelantamiento de la barrera punitiva para la creación de un delito obstáculo puesto que, reiteran, tal acceso en sí mismo no supone de por sí un comportamiento creador de un grave riesgo una multiplicidad de bienes jurídicos. Para ambas no nos hallamos ante un nuevo bien jurídico necesitado y merecedor de protección penal, sino que se trata simplemente del mismo bien jurídico que resulta atacado de forma desconocida. CORCOY BIDASOLO, 2007: 10. PUENTE ABA, 2004: 404-406.

[7] Por lo que se refiere al principio de intervención mínima, PUENTE ABA afirma que la incriminación de meras conductas de acceso ilegal en sistemas informáticos no respeta el carácter subsidiario y fragmentario del ordenamiento penal, pues no presenta la suficiente gravedad como para ser configurado como un tipo penal autónomo. Así, continua, no se verifican aquí los criterios que deben barajarse para juzgar si la intervención penal es proporcional y ajustada a la entidad del hecho. PUENTE ABA, 2004: 406-407.

[8] ROMEO rechaza la tipificación autónoma del hacking por entenderla perturbadora de las exigencias básicas de la prevención general con base en que, dada la escasa o nula capacidad de motivación del hacker, se incurriría en un Derecho penal puramente simbólico y promocional que genera una instrumentalización del individuo y una primacía, sin opción de equilibrio, de la eficacia sobre las garantías. MORÓN LERMA indica que *no parece oportuna la incriminación autónoma de las conductas de mero intrusismo informático, por revelarse como una huida al Derecho penal, con una intolerable cercenación de principios informadores y limitadores del ius puniendi*. En este sentido, considera que la prevención general no puede ser la justificación de la pena, ya que la justificación de al intervención del Derecho penal sólo desde el punto de vista de la prevención general acaba por comprometer el principio de proporcionalidad, y por otorgar primacía al principio de eficacia frente a las garantías. Por ello, afirma que *el recurso al Derecho penal en este caso cuestiona varios principios informadores del sistema penal, que no pueden desatenderse cuando se trata de postular la incorporación de un nuevo catálogo de conductas. No puede obviarse, en este punto, que esas otras conductas más peligrosas de las que las conductas de mero intrusismo serían antesala, resultan ya castigadas por diversos delitos que, de perpetrarse, absorben los accesos no autorizados. Por ello entiende que entran en conflicto con aspectos fundamentales de una política criminal racionalmente orientada cuyo respeto es condición previa de un Derecho penal legítimo*. MORÓN LERMA, 2002: 70, 78 y 83-85. ROMEO CASABONA, 1988: 40.

En la **jurisprudencia** la cuestión se tornaba más clara aunque no del todo uniforme. En este sentido, multitud de sentencias declararon atípicos comportamientos de acceso ilícito a un sistema informático y optaron por la absolución de los acusado. Pueden reseñarse al efecto las siguientes sentencias: Sentencia del Juzgado de lo Penal nº 2 Barcelona de 28 de mayo de 1999 (caso Hispanack), por falta de pruebas; la Sentencia de la Audiencia Provincial de Tarragona de 23 de julio de 2001; el Auto del Juzgado de Instrucción nº 2 Lorca de 29 de enero de 2002, la Sentencia de la Audiencia Provincial de Huelva 76/2006, de 16 de junio; la Sentencia del Tribunal Supremo 358/2007, de 30 de abril; y la Sentencia de la Audiencia Provincial de Córdoba 297/2008, de 28 de noviembre.

No obstante, excepcionalmente también se manejaron por los tribunales interpretaciones que abrían la puerta a sancionar determinadas conductas de intrusismo informático. Así pues, la alternativa a la absolución que declaraban las resoluciones judiciales anteriormente citadas debe añadirse la condena en aplicación del apartado 1 del artículo 197 del Código penal por parte de la Sentencia del Juzgado de lo Penal nº 2 Badajoz 42/2006, de 15 de febrero[9].

[9] Radical se mostraba la Sentencia del Juzgado de lo Penal número 2 de Badajoz, de 15 de febrero de 2006, que literalmente afirmaba *[s]i el hacker más allá de navegar por los circuitos de la red, llega a averiguar las claves de acceso al sitio, las quebranta y entra al lugar en que se alojan los circuitos protegidos por la clave averiguada descubre "los secretos" de otro. Las conductas desarrolladas por el intruso al lograr el quebrantamiento de las claves de acceso a los passwords ponen de manifiesto no sólo el dolo genérico de saber lo que se hace y la voluntad de hacerlo sino también el dolo y ánimo específico 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 impeditiva del pago al contenido que hay detrás de la misma. Bastará por ende para la consumación del delito de interceptación, entendiendo por tal el descubrimiento del password, independientemente de descubrimiento efectivo de la intrusión o secretos ajenos que se esconden detrás de la clave de acceso (que pertenecen a la fase de agotamiento delictual). Desde esta perspectiva la conducta es perfectamente encuadrable en el delito de descubrimiento y revelación de secretos del apartado 1 del artículo 197.*

No eran pocas, aun así, las voces que ponían de manifiesto la ausencia de un tipo penal adecuado para dar respuesta a los casos de acceso ilícito. De hecho, las opiniones a favor de la configuración autónoma del acceso ilícito fueron progresivamente siendo más numerosas hasta que, finalmente, fue mayoritaria la doctrina que identificaba el acceso ilícito como una infracción penal autónoma que no gozaba de protección específica en el Código penal y se manifestaba a favor de su incriminación[10].

Así, por ejemplo, RAGUÉS I VALLÉS y ROBLES PLANAS ponían de manifiesto que la normativa vigente sólo abarcaba una parte de las conductas de acceso no autorizado[11] afirmaba MATELLANES RODRÍGUEZ *que el acceso no consentido habrá de ser delito en todos los Estados... ha de haber una incriminación concreta para esta clase de conducta* porque entender que el acceso ilícito ya está castigado con otros delitos, su castigo se llevaría a cabo mediante la tentativa de estos otros delitos, hecho que implicaría incumplir su castigo como delito[12]. Otros autores como DE LA MATA BARRANCO, en cambio, aunque reconocían esta necesidad de tutela, reconducían la introducción del tipo al amparo de un bien jurídico tradicional[13].

---

[10] Muy expresivo es MORALES GARCÍA cuando pone de relieve que la decisión político criminal de tutelar o no penalmente el acceso ilícito sin otra finalidad es compleja, pero que asimismo se trata de *conductas cuyo desvalor es elevado, dada la naturaleza del acceso y/o los conocimientos especiales del autor. La punición del acceso abusivo, huérfano de cualquier otra finalidad por la que el legislador se ha decantado ahora no podía ser una alternativa 10 años atrás, pues habría significado un uso promocional del Derecho penal para la educación primaria de los usuarios, es decir, para la creación de una conducta colectiva de ilicitud del acceso.* MORALES GARCÍA, 2010: 184. MORALES GARCÍA, 2012: 152-153. Ver también FLORES PRADA, 2012: 11.

[11] RAGUÉS I VALLÈS et al., 2012: 371.

[12] MATELLANES RODRÍGUEZ, 2008: 60.

[13] En este sentido se manifiesta DE LA MATA BARRANCO cuando, en un estudio genérico sobre la conceptualización de la delincuencia informática, incluye entre las conductas que no encajan en precepto penal alguno, como puede ocurrir en la legislación penal española con el caso de los hackers inocuos o blancos y se decanta, finalmente, por introducirlas en el seno de los delitos contra la intimidad. DE LA MATA BARRANCO, 2010: 24. DE LA MATA BARRANCO y HERNÁNDEZ DÍAZ, 2010: 179.

Los motivos fundamentales en los que estos autores justificaron la introducción del acceso ilícito como un delito autónomo en el Código penal español fueron los siguientes:

a) Función de las nuevas tecnologías en la sociedad actual: la sociedad actual depende extraordinariamente de la utilización de los sistemas informático, que constituyen el principal medio de crecimiento económico y social[14]. Este hecho conduce a la necesidad de reconocer su valor social positivo como necesario y vinculante para un correcto desarrollo del sistema social[15].

b) Necesidad de armonización: la tipificación del acceso ilícito tiene su razón de ser en la necesidad de transponer dos normas de naturaleza supranacional, las antes referidas: el Convenio sobre Cibercriminalidad del Consejo de Europa, de 23 de noviembre de 2001, y la Directiva 2013/40/EU del Parlamento Europeo y del Consejo, de 12 de agosto de 2013, relativa a los ataques a sistemas de información. La armonización se presenta en este sentido como necesaria a los efectos de aunar esfuerzos para luchar contra este tipo de delincuencia desde los ámbitos internacional y comunitario debido a las especiales características de comisión de tales conductas, especialmente el carácter transfronterizo de las mismas[16].

c) El hecho de que el acceso ilícito constituye la antesala de delitos más graves: la potencialidad multiplicadora de las acciones ilícitas derivadas del acceso ilícito así como el especial peligro o vulnerabilidad que la propia conducta crea para multitud de bienes jurídicos[17].

---

[14] RUEDA MARTÍN, 2010: 376-377.

[15] RUEDA MARTÍN, 2010: 376-377.

[16] COUNCIL OF EUROPE, 2001: 11 párrafo 34. RUEDA MARTÍN, 2010: 376-377.

[17] CARRASCO ANDRINO, 2010a: 344. MIR PUIG, 2002: 301. ROMEO CASABONA, 2006: 1 y ss.

Harto sorprendente resulta el hecho de que la Directiva y, algún sector de la doctrina española[18] ofrecen como justificación de la intervención penal en este ámbito motivos relacionados con la prevención de la delincuencia organizada[19] en lugar de referir razones vinculadas al propio fenómeno informático, tal y como, por ejemplo, realizan el Convenio o la Decisión Marco, así como toda la normativa internacional anteriormente aprobada.

La Unión Europea se desvía con ello del verdadero propósito que tienen los distintos mandatos incriminatorios, adoptando una política excesivamente restringida y volcada únicamente en de las distintas parcelas que integran la delincuencia informática, el terrorismo y las infraestructuras públicas, dejando de lado un amplio espectro de intereses legítimos dignos de protección frente a la utilización y el desarrollo de las tecnologías de la información, como son las empresas y los particulares. En cualquier caso, esta concepción tan *limitada* no ha sido acogida por ningún Estado y tampoco por la doctrina mayoritaria[20], quienes han afrontado la transposición de dichas normas desde una visión global de este fenómeno. Esta concepción más "neutra" será también la defendida en el presente estudio.

---

[18] Así, citando el Considerando (3) de la propia Directiva, ponen de relieve CASTIÑEIRA PALOU y ESTRADA I CUADRAS que los fines político-criminales perseguidos con la criminalización del acceso ilícito persiguen, básicamente, luchar contra la posibilidad de ataques terroristas o de naturaleza política contra los sistema de información que forman parte de las infraestructuras críticas de los Estados miembros y de la Unión. Por infraestructuras críticas refiere la Directiva en su Considerando (4) aquellas que son esenciales para para el mantenimiento de funciones vitales de la sociedad, la salud, la seguridad, la protección y el bienestar económico y social de la población, como las centrales eléctricas, redes de transporte y las redes de los órganos de Gobierno. Estos autores proponen una interpretación teleológica del tipo orientada hacia esta perspectiva más restringida, afirmando que una interpretación abierta atenta contra el principio de proporcionalidad. CASTIÑEIRA PALOU y ESTRADA CUADRAS, 2015: 163.

[19] En igual sentido, FERNÁNDEZ TERUELO, 2011: 195-196.

[20] Entre otros, ANARTE BORRALLO y DOVAL PAÍS, 2015: 511 y ss. CARRASCO ANDRINO, 2010, CARRASCO ANDRINO, 2010, RUEDA MARTÍN, 2010, FERNÁNDEZ TERUELO, 2011.

B) ÁMBITO OBJETIVO DE LA INVESTIGACIÓN

Presentado el tema y justificada la importancia de su tratamiento, considero oportuno ahora caracterizar brevemente el delito que nos ocupa definiendo el acceso ilícito desde un punto de vista objetivo, centrando la cuestión de forma directa en cuáles eran las pretensiones supranacionales de incriminación y en cuál es el desarrollo que el legislador español ha hecho de las mismas en nuestro ordenamiento jurídico. Ello permitirá al lector adquirir una rápida visión del objeto de estudio.

1. OBJETO DE ESTUDIO

La Directiva y el Convenio imponen la obligación a los Estados miembros/parte de tipificar como delito la acción de acceder ilícitamente a todo o parte de un sistema informático (*the access to the whole or any part of a computer system without right,* añade la Directiva, *by the infringement of security measures*) como medio para proteger en un primer estadio el contenido de dichos sistemas. Como puede observarse, conforme al mandato incriminatorio previsto en la normativa supranacional el acceso ilícito puede expresarse en tres ideas:

a) Es una conducta que consiste en un mero acceso ilícito a un sistema informático (con vulneración de medidas de seguridad).

b) Es un comportamiento que no ocasiona daños en el sistema, programa o datos informáticos objeto de acceso.

c) Subjetivamente, el autor no busca otra cosa que el mero acceso (dolo directo), actuando sin voluntad de acceder ni descubrir datos o secretos, ocasionar un perjuicio patrimonial y, menos aún de producir ningún género de deterioro o destrucción de los datos del o del propio sistema (no la informa la voluntad del autor ninguna tendencia subjetiva interna o elemento subjetivo del injusto).

En España la introducción de esta conducta tuvo lugar en 2010 a través de la Ley Orgánica 5/2010, de 22 de junio. De las distintas vía de incriminación posibles, el legislador escogió la formulación de un tipo de equivalencia con el delito de descubrimiento y revelación de secretos en el apartado 3 del artículo 197 en el Título dedicado, por tanto, a los delitos contra la intimidad[21]. La ubicación sistemática del tipo así como la configuración de los distintos elementos de éste conducían a negar el carácter de anticipación de la tutela penal del delito y distorsionaba su ámbito aplicativo[22]. No cabía sino concluir el carácter defectuoso de la transposición que el legislador había efectuado de la normativa supranacional citada y hacía surgir la necesidad de reformarla.

En 2015, la redacción típica del delito fue modificada por la Ley Orgánica 1/2015, de 30 de marzo, de tal forma que ahora se adapta mejor a las exigencias supranacionales, siendo posible mediante una correcta interpretación hermenéutica el cumplimiento de su mandato. El delito de acceso ilícito se configura ahora como un tipo autónomo en el apartado 1 del artículo 197 *bis* del Código penal que puede ahora cumplir las expectativas de protección del sistema informático[23].

---

[21] El tenor de dicho precepto rezaba: *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.*

[22] El legislador español había forzado desmesuradamente la norma más allá de los límites de la justificación penal. Como se verá, el aspecto más flagrante de incoherencia e incorrección legislativa se manifiesta ya en la propia ubicación sistemática, que obligó al legislador a modificar el objeto material del delito y, con ello, el resto de los elementos típicos para adaptarlos al bien jurídico protegido que se pretendía atribuir al acceso ilícito a un sistema informático: la intimidad.

[23] Este precepto reza: *1. 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.*

2. LIMITACIÓN DEL OBJETO DE ESTUDIO

En cualquier caso, el artículo 197 *bis* se integra, además del apartado primero, por un segundo apartado al que no se prestará más que una atención sesgada y colateral en este trabajo[24]. La razón de lo anterior estriba en que, en mi opinión, las dos conductas previstas respectivamente en los apartados 1 y 2 del artículo 197 *bis* son totalmente independientes[25]. La primera castiga el acceso ilícito a un sistema informático y, la segunda, la interceptación de transmisiones de datos no públicas. Dicha divergencia se manifiesta, específicamente, en los siguientes aspectos,

> **a) Naturaleza jurídica:** la interceptación y el acceso ilícito fueron conductas inicialmente previstas como alternativas en el primer texto con el cometido de incriminar comportamientos en los que se veía involucrado un sistema informático como alternativos: *Computer-related crime – Analysis of legal policy de 1986*, siendo separadas por la Recomendación 89 (9), del Consejo de Europa, adoptada el 13 de septiembre de 1989, sobre delincuencia informática, debido a su diferente naturaleza, —la primera dirigida a proteger las comunicaciones y la segunda el sistema informático—, escisión que se ha mantenido posteriormente[26].

---

[24] Mediante esta nueva conducta se tipifica la utilización de artificios o instrumentos técnicos para interceptar transmisiones "no públicas" de datos informáticos. El apartado 2 del artículo 197 *bis* reza: *2. El que mediante la utilización de artificios o instrumentos técnicos, y sin estar debidamente autorizado, intercepte transmisiones no públicas de datos informáticos que se produzcan desde, hacia o dentro de un sistema de información, incluidas las emisiones electromagnéticas de los mismos, será castigado con una pena de prisión de tres meses a dos años o multa de tres a doce meses.*

[25] Aun teniendo en cuenta lo anterior, aunque como señala de forma unánime la escasa bibliografía existente en la materia, , los principales conflictos interpretativos de este segundo apartado no se presentan en relación con el apartado 1 del 197 *bis*, el acceso ilícito, sino con respecto al propio tipo básico de descubrimiento y revelación de secretos, me veo obligada a analizar las diferencias existentes entre uno y otro apartado del precepto. Concretamente, estas diferencias son las siguientes: COLÁS TURÉGANO, 2013: 222 y ss.

[26] El Informe consideraba que el avance de la tecnología hacía cada vez más difícil distinguir entre sistemas de telecomunicación e informáticos. OCDE, 1986: 60.

b) Bien jurídico protegido: mientras que el acceso conforma una infracción de carácter básico dedicada a impedir cualquier tipo de intromisión en el sistema informático y, en consecuencia protege la seguridad informática[27], la interceptación de transmisiones no públicas de datos tiene como finalidad específica proteger el derecho a la privacidad de las comunicaciones de datos[28] o, lo que conoceríamos en España como derecho al secreto de las comunicaciones[29].

c) Acción: la acción sobre la que se proyecta la conducta es distinta en uno y otro apartado. La acción de acceso supone una introducción electrónica en un sistema informático o en parte del mismo, pero no incluye el acceso a datos en

---

[27] COUNCIL OF EUROPE, 2001: 13 párrafo 44-45.

[28] COUNCIL OF EUROPE, 2001: 15 párrafo 51-52.

[29] La interceptación no autorizada de transmisiones de datos vendría a castigar una nueva modalidad de intromisión clandestina en una telecomunicación privada, lo que supone, como muy bien indica COLÁS TURÉGANO, la interferencia en una de comunicación de cualquier clase y no en una comunicación íntima como se venía castigando hasta ahora. En este sentido, mientras el apartado 1 del artículo 197 del Código penal castiga la interceptación de las comunicaciones vinculadas a la intimidad, este precepto sí vendría a proteger el derecho al secreto de las comunicaciones. Como expondrá más adelante, el apartado 1 del artículo 197 castiga las vulneraciones de la intimidad derivadas de la interceptación de las comunicaciones, pero el derecho al secreto de las comunicaciones tiene un contenido más amplio y diferenciado del derecho a la intimidad. El derecho al secreto de las comunicaciones tiene una naturaleza puramente formal basada en la presunción *iuris et de iure* de que todo lo comunicado es secreto con independencia del contenido material de lo comunicado. En cambio, el derecho a la intimidad, que es lo que se protege en el apartado 1 del artículo 197, tiene un carácter material que no se centra en el proceso de comunicación sino en el contenido de la propia comunicación. Este último derecho sería el protegido en el apartado 1 del artículo 197 mientras que el propio derecho al secreto de las comunicaciones en sí mismo considerado sería el bien jurídico protegido en el apartado 2 del artículo 197 bis. A favor, COLÁS TURÉGANO, 2015: 223. Véase también, RUIZ MIGUEL, 1995: 89. BOIX REIG, 1989: 19. ELVIRA PERALES, 2007: 22. RODRÍGUEZ LAINZ, 2011: 205. MARTÍN MORALES, 1995: 40.

transmisión[30]. Así pues, acceder comprenderá, meramente, la introducción en un sistema localizado en algún lugar del planeta, mientras que la interceptación se producirá entretanto tiene lugar el proceso de comunicación, esto es, en el periodo que va desde el inicio de la emisión de la comunicación hasta el fin de esta mediante su recepción en el sistema informático, pero nunca cuando la comunicación ha llegado a su destino (el interior, si se quiere, del sistema informático)[31].

d) Objeto material: el objeto material de uno y otro son distintos. Mientras que en el acceso ilícito es el sistema informático, en la interceptación ilícita son los datos

---

[30] Así mismo se desprende del propio Informe explicativo de la Convención de Cibercrimen, que en su párrafo 44 explica: *"Access" comprises the entering of the whole or any part of a computer system (hardware, components, stored data of the system installed, directories, traffic and content-related data). However, it does not include the mere sending of an e-mail message or file to that system. "Access" includes the entering of another computer system, where it is connected via public telecommunication networks, or to a computer system on the same network, such as a LAN (local area network) or Intranet within an organisation. The method of communication (e.g. from a distance, including via wireless links or at a close range) does not matter.* En consecuencia, el sistema de comunicación no tiene relevancia alguna para el acceso, pudiendo también la entrada tener lugar mediante el contacto físico del autor con el sistema. En cualquier caso, si el acceso se produce por vía remota mediante la conexión a una vía pública o privada de comunicación —debe tenerse en cuenta que el apartado 2 solo incluye comunicaciones privadas—, ésta tan solo será el medio de comisión del delito. COUNCIL OF EUROPE, 2001: párrafo 44.

[31] Será interceptación, conforme a esta idea, la desviación de un correo electrónico hacia una máquina controlada por el sujeto activo durante el periodo de transmisión. ROMEO CASABONA, de hecho, define interceptación como la intromisión cognoscitiva en comunicaciones ajenas. El propio Consejo de Europa indica en el Informe que el término interceptación está relacionado con las comunicaciones o transmisiones de datos así como con las radiaciones electromagnéticas que, dentro de éstas, pueden servir para descubrir tales datos. Se refiere, pues, a escuchar, monitorear o vigilar el contenido de las comunicaciones, a adquirir los contenidos de datos de dichas comunicaciones o a la grabación de la mismas. Se trata de cualquier forma de transferencia electrónica de datos, ya sea por teléfono, fax, correo electrónico o transferencia de archivos, hecho éste último que incluye la interceptación de datos que están siendo enviados dentro de la red electrónica que integra el propio sistema informático, como, por ejemplo, desde el ordenador a la impresora. FERNÁNDEZ TERUELO, 2007: 124. ORTS BERENGUER y ROIG TORRES, 2001: 25. ROMEO CASABONA, 2004b: 88 y 95. COUNCIL OF EUROPE, 2001: párrafos 51 a 58.

informáticos[32]. Efectivamente, aunque con la reforma de 2010 el objeto material del delito de acceso ilícito a un sistema informático eran los datos contenidos en un sistema informático, con acierto, en mi opinión, este elemento del tipo fue modificado para fijar la atención correctamente como objeto del acceso ilícito en el sistema informático. Desde 2015, pues, interceptación de transmisiones no públicas de datos y acceso ilícito no comparten ya este elemento del tipo.

[32] El acceso ilícito pretende, pues, sancionar la intrusión en un sistema informático ajeno sin prestar atención a su contenido, en la medida en que éste puede ser muy variado: desde la cartera de clientes de una empresa, hasta la obra de ingenio de una persona —la tesis misma—, como fotos privadas y personales, cuyo apoderamiento supondría graves perjuicios unas veces económicos y otros personales para el titular de los mismos. La tutela se dirige, en este sentido, no al contenido sino al continente como medio para evitar la agresión de los múltiples intereses en juego.

II. JUSTIFICACIÓN DE LA ELECCIÓN E IMPORTANCIA DEL TEMA

Teniendo en cuenta lo anterior, la importancia del presente trabajo radica en tres aspectos:

a) Novedad del tema: En primer lugar, en la extrema novedad del tema que en él se trata. El acceso ilícito conforma, a día de hoy, una conducta con unos contornos interpretativos difusos u carente de un desarrollo doctrinal. Por este motivo, resulta necesario asentar una base jurídica sólida que sirva como guía tanto para un posterior desarrollo doctrinal como para resolver las posibles dudas que puedan presentarse a los prácticos del Derecho en la aplicación del tipo.

b) Ausencia de una base jurídico penal sobre la que instaurar las conductas informáticas: En segundo lugar, en que la ausencia de una tradición incriminatoria en la materia motiva la necesidad de crear una base jurídico-penal que permita asentar los cimientos —hoy ausentes— en nuestro Código penal para la inclusión posterior de cualquier infracción penal vinculada a la informática que pueda surgir en el futuro o cuya incardinación actual pueda resultar sino atípica, al menos controvertida. Y para ello resulta muy propicia la conducta de acceso ilícito, puesto que conforma la amenaza informática más básica en el seno del fenómeno conocido como delincuencia informática que actúa como barrera previa de protección de otros bienes jurídicos anticipando la tutela penal a un estado previo.

c) Carácter pionero del estudio: debe señalarse que, por el momento, no existe una monografía expresamente dedicada al acceso ilícito, algo que se apoyado por la escasa bibliografía española en la materia así como el contado número de sentencias aprobadas. Creo que ésta también es una razón que, aunque con menor peso, justifica la realización del presente estudio.

III. METODOLOGÍA Y OBJETIVOS

Teniendo en cuenta lo anterior, mi tesis va encaminada a arbitrar los mecanismos adecuados para lograr la correcta incriminación de la conducta de acceso ilícito a un sistema informático y, con ello, asentar los cimientos —hoy ausentes— en nuestro Código penal para la inclusión posterior de cualquier infracción penal vinculada a la informática que pueda surgir en el futuro o cuya incardinación actual pueda resultar sino atípica, al menos controvertida, como por ejemplo, DoS (SYN Flood, ICMP y Smurfs Attacks), Pings (Dead Ping, Ping Flooding, etc.), wiretapping, Replay Attacks, MiTM, 0-day-attack, Trashings, monitoring, entre otros. A este efecto, mi investigación se desarrolla desde una triple perspectiva:

a) En primer lugar, sistemática, teniendo en cuenta la ubicación sistemática del delito y su relación con los distintos tipos del Código penal en relación con los cuales resulta necesaria su interpretación a los efectos de dotarlo de contenido.

b) En segundo lugar, doctrinal y jurisprudencial, tomando como especial punto de referencia las distintas corrientes existentes para el análisis hermenéutico del tipo penal estudiado y de aquellos con los que tiene relación.

c) En tercer lugar, comparada, sobre la base del estudio de la normativa penal existente en otros países con un importante recorrido legislativo en este fenómeno delictivo teniendo en cuenta las opiniones vertidas en la literatura comparada para la interpretación de los distintos términos legales en cada una de las respectivas legislaciones estudiadas.

d) En último lugar, en el ámbito supranacional, pues la armonización penal es el fin de la introducción del tipo.

PRIMERA PARTE
NORMATIVA INTERNACIONAL
Y COMPARADA

CAPITULO I

LA ARMONIZACIÓN SUPRANACIONAL DEL ACCESO ILÍCITO EN LAS ORGANIZACIONES DE CARÁCTER SUPRANACIONAL

I. INTRODUCCIÓN

En este primer Capítulo se contienen, a modo de introducción histórico-legislativa, los principales hitos normativos de carácter supranacional (esto es, tanto a nivel internacional como comunitario) a través de los que, durante décadas, se ha puesto de relieve la necesidad de incriminar el acceso ilícito a un sistema informático. La presentación de las distintas disposiciones normativas se realizará siguiendo un orden cronológico, ya que, en mi opinión, este criterio permitirá al lector apreciar mejor dónde y cómo surgió la necesidad de sancionar penalmente esta conducta, cuando tuvo lugar su primera propuesta de incriminación y cómo ha sido de ésta posterior evolución hasta la actualidad.

El camino se iniciará, en este sentido, con la consideración de la criminalidad informática como una hipótesis de no Derecho, es decir, como un fenómeno en el que no es necesaria la intervención jurídica por estar dotado de autorregulación propia. Posteriormente, se verá como el auge que las nuevas tecnologías adquieren en el ámbito empresarial propiciará en la década de los 80 el surgimiento de una tímida pretensión incriminatoria de diversas conductas de naturaleza informática en el seno de la delincuencia económica. Progresivamente, este propósito se irá reforzando y extendiendo a ámbitos de tutela distintos al patrimonial, poniéndose de relieve el carácter imprescindible de una armonización penal nacional en la materia, armonización que finalmente se logrará, después de varios intentos frustrados (debido a la naturaleza meramente recomendatoria de las normas aprobadas al efecto), con la adopción de dos disposiciones de carácter vinculante:

a) El Convenio sobre la Ciberdelincuencia, del Consejo de Europa, firmado en Budapest el 23 de noviembre de 2001, y

b) 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.

Estas dos normas gozan de una importancia capital por lo que respecta a la consecución del objetivo comentado, ya que han conseguido que los Estados que todavía no habían criminalizado ciertos comportamientos vinculadas a la informática aprobaran la legislación oportuna en la materia. Esta idea es especialmente aplicable a nuestro país, porque, de hecho, su aprobación es la única razón que *a priori* parece haber motivado la tipificación en España del delito de acceso ilícito objeto del presente trabajo[1].

Por último, debe reseñarse que, aunque todas las normas a las que se hará referencia proponen la tipificación expresa de un conjunto de conductas de distinta naturaleza vinculadas a la informática en tanto mínimo imprescindible para la lucha contra esta forma de delincuencia, se obviará el análisis de aquellos comportamientos que no contribuyen al propósito del presente trabajo (el análisis dogmático del acceso ilícito a un sistema informático), con el fin de evitar una innecesaria prolongación del texto así como la introducción de cuestiones que no vendrían al hilo de este objeto.

En consecuencia, serán objeto de comentario, solamente, el acceso ilícito a un sistema informático y el uso no autorizado del sistema, base, esta última, para la incriminación del mantenimiento ilícito en un sistema informático, hoy conducta alternativamente castigada en el apartado 1 del artículo 197 *bis* (antiguo 197.3) No se tratará, por tanto, la interceptación de transmisiones no públicas de datos, tipificada en el apartado 2 del mismo precepto, pues, como se ha indicado en el objeto de estudio, aunque inicialmente está conducta integraba un tipo mixto alternativo con el acceso ilícito, pronto se vio la inmensa diversidad existente en la configuración del injusto en una y otra, diversificándose su propuesta de incriminación y proponiéndose como un tipo autónomo.

Sin más preámbulos, paso a dicho análisis.

---

[1] Así se expresó en la Exposición de Motivos de la Ley Orgánica 5/2010, de 22 de junio.

II. OCDE: EL INFORME *COMPUTER-RELATED CRIME*

La delincuencia informática nació en el seno de la criminalidad económica. Concretamente, fue en la *12th Conference of Directors of Criminologidal Reserch Institutes: Criminological Aspects of Economic Crime* del Consejo de Europa, celebrada en el año 1976 en Estrasburgo, donde se debatió por primera vez si se debía o no ofrecer una respuesta penal a todo un amplio abanico de delitos económicos cuya comisión comenzaba a ser reiterada a través de la informática[2]. Casi al mismo tiempo, sin embargo, en el Congreso celebrado en Liège en 1977 se planteaba la posibilidad de considerar este nuevo fenómeno como una hipótesis de no Derecho, esto es, un supuesto dotado de autorregulación propia[3].

Si bien inicialmente ciertos ilícitos relacionados con la informática podían hallar sanción en el marco de los denominados delitos económicos, paulatinamente el cerco de conductas de deseable punición se fue ampliando más allá de la delincuencia económica hasta convertirse en un fenómeno de devastadores consecuencias. Fue entonces cuando, ya entrada la década de los 80, la Organización de Cooperación y Desarrollo Económico (OCDE) creó un Comité de Expertos en Delincuencia Informática con el objeto de identificar cuáles eran los comportamientos propiamente informáticos y analizar las posibilidades de lograr una armonización del Derecho penal a nivel internacional en la materia.

---

[2] SCHJOLBERG, 2008: online.

[3] Efectivamente, este mismo debate se suscitó en el Congreso celebrado en Liège en 1977, donde se planteó la posibilidad de que la informática e, igualmente, el fenómeno incipiente que todavía constituía Internet pudieran integrar fenómenos de no derecho caracterizados por su propia autorregulación. Todo ello a la sazón de la publicación del libro *L'hypothese de non droit* por parte de Jean Carbonnier el año 1963. CARBONNIER, 1963: 33-63. Traducción CARBONNIER, 1974: 33-63.

El resultado del estudio llevado a cabo por dicho Comité fue el Informe *Computer-related crime – analisys of legal policy* de 1986, en el que éste sugirió la adopción de medidas en relación con una lista de cinco actos que consideró el común denominador para el acercamiento de las respectivas legislaciones. Concretamente, en el quinto número de dicha lista incluyó *el acceso o la interceptación de un ordenador y/o sistema de telecomunicaciones realizados dolosamente y sin la autorización de la persona responsable del sistema, bien infringiendo medidas de seguridad, o bien por cualquier otra finalidad deshonesta o dañina*[4].

Aunque el Informe supone la plasmación escrita de la perspectiva informático-económica inicialmente apuntada —al atribuir una naturaleza puramente patrimonial a los ilícitos vinculados con la informática[5]—, su importancia radica, en mi opinión, en que constituye el primer texto que hace referencia a la delincuencia informática como un fenómeno criminal con entidad propia (*computer related-crime)*, y que aúna los comportamientos más graves e injustos relacionados con la misma, recogiendo entre ellos el aquí estudiado acceso ilícito a un sistema informático. Se trata, por tanto, de la primera propuesta de incriminación y configuración legal del delito objeto de estudio.

---

[4] "*5. The access to or the interception of a computer and/or telecommunication system made knowingly and without the authorization of the person responsible for the system, either (i) by infringement of security measures or (ii) for other dishonest or harmful intentions."* OCDE, 1986: 65, 70.

[5] El Informe entiende que la materia prima de los sistemas informáticos es la información y que ésta está adquiriendo un valor económico cada vez mayor hasta el punto de haberse convertido en un poderoso activo negociable, considerando susceptibles de sanción penal algunos de los comportamientos informáticos a través de los delitos contra la propiedad. Sin embargo, el Informe no es ajeno a las posibilidades de ataque que representa la informática para otros derechos, como la privacidad, cuyas posibilidades de afectación no analiza al considerar que ello ya ha sido objeto de otros estudios previos tanto por parte de la propia Organización (*Guidelines governing the protection of privacy and transborder data flows of personal data de 30 de septiembre de 1980*) como por parte de otras organizaciones internacionales como el Consejo de Europa (*Convention for the protection of individuals with regard to automatic processing of personal data, en vigor desde el 1 de octubre de 1985*). OCDE, 1986: 29. OCDE, 1986: 23.

De los comportamientos cuya tipificación analiza, no solo resulta de interés a los efectos del presente estudio el acceso ilícito a un sistema informático, sino también el uso no autorizado de un ordenador —a cuyo análisis se dedica una parte del Informe aunque finalmente se llega a incluir entre las propuestas específicas de incriminación que efectúa en la parte final[6]—, conducta que constituirá la base jurídica para la posterior incriminación por parte de Italia, Francia y España del mantenimiento ilícito en un sistema informático[7]. Véase cada una de ellas por separado:

A) USO NO AUTORIZADO DE UN ORDENADOR

El uso no autorizado de un ordenador es concebido por el Informe de forma análoga a la utilización inconsentida de un bien cuya propiedad pertenece a otra persona, aunque en este caso el objeto material del delito se despliega en torno a un doble ámbito: un bien intangible, es decir, la información, y distintos elementos físicos, esto es, el hardware que integra ordenador[8].

1. JUSTIFICACIÓN Y VÍAS PARA SU INCRIMINACIÓN

La justificación de su criminalización se halla, en opinión del Comité, en la potencial dañosidad y en el riesgo para el propietario del ordenador puede entrañar este comportamiento[9]. Sin embargo, no lo incluye entre las cinco conductas cuya tipificación se recomienda en las propuestas finales, en parte por considerar que un buen número de supuestos (o, al menos, los más graves) de uso no autorizado son susceptibles de ser subsumidos en el acceso ilícito[10].

---

[6] OCDE, 1986: 59-60.

[7] Ello sin perjuicio de lo que más tarde se dirá respecto a la conducta de exceso de autorización que aparece recogida en la Sección 1030 del Código penal federal de Estados Unidos de América. Para más información, véase Capítulo II.

[8] OCDE, 1986: 56.

[9] OCDE, 1986: 56.

[10] OCDE, 1986: 56.

Aunque no recomienda su incriminación como hace con el acceso ilícito, el Informe menciona las vías que consideraría más adecuadas para que los legisladores nacionales incorporasen esta conducta en sus respectivos ordenamientos jurídico-penales[11]. Específicamente, las dos siguientes:

> a) La creación de una previsión general sobre desposesión ilegal o uso de la propiedad de otro, o
>
> b) La introducción de un tipo autónomo relativo al hurto de uso de sistemas informáticos conforme a las siguientes posibilidades:
>
> > i) Como una cláusula general aplicable a todas las conductas de naturaleza informática;
> >
> > ii) Como un tipo de equivalencia en relación con otro tipo penal ya existente como el uso no autorizados de telecomunicaciones;
> >
> > iii) o, finalmente, como una previsión específica.

2. BIEN JURÍDICO PROTEGIDO

Por último, apunta como bien jurídico protegido en este delito al valor que tiene el uso exclusivo de los sistemas de información computarizada por su propietario sin interferencias por parte de terceros ajenos[12].

---

[11] En cualquier caso, si el legislador nacional decide finalmente tipificar la conducta, el Informe entiende que deben excluirse del ámbito típico del precepto aquellos supuestos en los que el uso no autorizado del ordenador se comete con la intención de perpetrar otro delito informático (caso hipotético en el que, según el Derecho español, el uso no autorizado quedaría absorbido por este último en aplicación de la regla 3ª del artículo 8 del Código penal) así como la finalidad que se pretende conseguir sea la causación de un daño (caso que igualmente se resolvería en virtud del principio de consunción), y aconseja especial cautela en la definición del delito cuando éste se comete en el seno de una relación empresarial entre empleador y empleado. OCDE, 1986: 59.

[12] OCDE, 1986: 56.

B) ACCESO NO AUTORIZADO

1. BIEN JURÍDICO PROTEGIDO

El Informe considera como un interés necesitado de tutela la salvaguarda de la integridad del propio sistema de almacenamiento de la información con independencia de la naturaleza de ésta, ello en atención al potencial peligro que puede entrañar para otros bienes el incremento de la frecuencia de los accesos no consentidos por vía remota a sistemas de procesamiento de datos[13].

2. PARTE OBJETIVA Y SUBJETIVA DEL TIPO

La conducta de acceso ilícito aparece vinculada como un tipo mixto alternativo a la de interceptación de telecomunicaciones[14]. A este respecto prevé la posibilidad de limitar la esfera de aplicabilidad del precepto mediante la introducción de dos restricciones, una en el tipo objetivo: la infracción de medidas de seguridad, y otra en el tipo subjetivo: la sanción únicamente de la modalidad dolosa. En cualquier caso, la consumación del acceso se produce con la mera penetración en el sistema, sin necesidad de causar daño alguno[15].

Además, recomienda la introducción de una claúsula premial (sin especificar la naturaleza que debe tener esta cláusula, por ejemplo, de excusa absolutoria o como subtipo privilegiado) aplicable a aquellos casos en los que se de inmediata noticia del acceso y de las lagunas del sistema accedido[16].

---

[13] Esta idea —el distinto carácter de la información almacenada— justifica, pues, para el Comité que sea el continente y no el contenido al que vaya referida la protección, así como su tipificación separada de los delitos relativos a la privacy y a las distintas esferas del secreto. OCDE, 1986: 63.

[14] Considera que existe una imposibilidad manifiesta de deslindar esta conducta de la interceptación de telecomunicaciones en la medida en que opina que el avance de la tecnología hace cada vez más difícil distinguir entre sistemas de telecomunicación y sistemas informáticos. OCDE, 1986: 60.

[15] Hecho que el Comité asimila a la copia la una llave de entrada a una propiedad y/o el posterior acceso a la misma de conformidad con la comentada naturaleza patrimonial que atribuye al ilícito. OCDE, 1986: 61.

[16] OCDE, 1986: 63.

III. CONSEJO DE EUROPA: RECOMENDACIÓN 89 (9), DE 13 DE SEPTIEMBRE, SOBRE DELINCUENCIA INFORMÁTICA

El Informe *Computer-related crime – analisys of legal policy* constituyó un avance de capital importancia en lo que concernía al análisis jurídico-penal del emergente fenómeno que en aquel momento conformaba la delincuencia informática. En este sentido, sentó las bases sobre las que posteriormente se realizaría el desarrollo normativo de los ilícitos informáticos en el ámbito penal, que tendría lugar en el seno del Consejo de Europa y que se materializaría el 13 de septiembre de 1989 en la Recomendación 89 (9), sobre delincuencia informática, primera norma de carácter no vinculante aprobada por dicha organización en la materia.

La Recomendación propuso la incriminación de todas las conductas que se analizaban en el Informe (tanto las incluidas en la lista final como las meramente analizadas y de las que no se realizaba propuesta de tipificación alguna), distinguiendo, no obstante, dos listas, una de mínimos[17], —que se correspondió con la lista recomendatoria final del Informe y en la que se recogieron aquellas conductas cuya elevada nocividad hacía necesaria su incriminación —, y otra de máximos, complementaria a la anterior y de carácter opcional —que incluía una serie comportamientos cuya escasa incidencia práctica no convertía por el momento en imprescindible su criminalización pero en relación con los cuales era previsible un considerable aumento de su comisión en el futuro, razón que motivaba, todavía, el carácter meramente opcional de la propuesta de tipificación respecto de las mismas—[18].

---

[17] Concretamente, en esta listas se incluían las siguientes conductas: fraude informático, falsificación informática, daños a datos o programas informáticos, sabotaje informático, acceso no autorizado, interceptación no autorizada, reproducción no autorizada de un programa informático protegido y reproducción no autorizada de la topografía. Para una mayor concreción sobre este punto, véase BEQUAI, 1990: 33.

[18] En ellas se enumeran la alteración de datos o programas informáticos, el espionaje informático, el uso no autorizado de un ordenador y el uso no autorizado de un programa de ordenador protegido. BEQUAI, 1990: 33.

El acceso ilícito a un sistema informático continuó en el quinto puesto de la lista de mínimos (al igual que el Informe): *acceso ilícito a un sistema informático o red de telecomunicaciones infringiendo medidas de seguridad*[19]. El Comité redactor de la Recomendación reafirmó con ello su convencimiento de que se trataba de una conducta *in crescendo* y potencialmente peligrosa[20], a consecuencia de que de su comisión podía (y puede) derivarse la creación brechas en la seguridad del sistema o la destrucción del contenido de éste por negligencia[21].

Efectuando un análisis comparativo con el Informe, en ella se introdujeron las importantes novedades que se detallan a continuación:

A) ACCESO ILÍCITO A UN SISTEMA INFORMÁTICO

1. BIEN JURÍDICO

Aunque la Recomendación considera en cierta medida la delincuencia informática como parte integrante del *white collar crime*[22], reconoce la existencia de nuevos intereses jurídicos que requiere la protección del Derecho penal[23]. A tal efecto, concibe la conducta de acceso como una figura delictiva con autonomía propia dirigida a proteger en primera instancia la seguridad del sistema o red informáticos (expresada ésta en la inviolabilidad del domicilio informático) y, de forma mediata, los intereses tutelados en los demás ilícitos cuya incriminación se propone y que presupone para su consumación la existencia de una previa intrusión en el sistema informático[24].

---

[19] *Unauthorized access. The access without right to a computer system or network by infringing security measures*.

[20] BEQUAI, 1990: 51.

[21] BEQUAI, 1990: 50.

[22] BEQUAI, 1990: 18.

[23] Tales como la disponibilidad de los medios de almacenamiento, procesamiento y transferencia de datos, la integridad del sistema informático y de los datos que éste contiene, y la confidencialidad de ciertos datos. BEQUAI, 1990: 23.

[24] Específicamente daños informáticos y espionaje informático. BEQUAI, 1990: 51.

2. PARTE OBJETIVA DEL TIPO

La Recomendación confiere un contenido más concreto a la conducta de acceso ilícito, que se manifiesta en los tres aspectos que se detallan a continuación.

a) ACCIÓN TÍPICA

En primer lugar, desglosa el acceso ilícito de la de interceptación de telecomunicaciones, previendo ambos comportamientos de forma separada[25]. La conducta se integra desde entonces por una única acción, la de acceder ilícitamente de forma total o parcial al sistema o red infringiendo medidas de seguridad[26].

b) OBJETO MATERIAL DEL DELITO

En segundo lugar, deslinda los dos objetos materiales sobre los que, una vez desvinculada de la conducta de interceptación, puede recaer la acción de acceso: el sistema informático (*informatic system)* y la red de telecomunicaciones (*network*), esto es, un complejo de dos o más ordenadores interconectados entre sí. La previsión de ambos elementos como objeto material permite entender englobadas tanto las comunicaciones internas como las externas y, al mismo tiempo, desglosarlas del concepto de sistema de telecomunicaciones (*telecommunication system*)[27].

---

[25] La conducta de interceptación no autorizada (*unauthorized interception*) se describe como *[l]a interceptación, realizada ilícitamente y utilizando medios técnicos, de comunicaciones dirigidas, recibidas o internas de un sistema informático o una red de ordenadores*. [*Unauthorized interception. The interception, made without right and by technical means, of Communications to, from and within a computer system or network.]*

[26] BEQUAI, 1990: 52.

[27] A tal efecto, distingue las conductas que afectan a los datos o programas informáticos (*computer fraud, computer forgery, damage to computer data or computer programs, computer sabotage, alteration of computer data or computer programs, unauthorized reproduction of a protected computer program* y *unauthorized use of a protected computer program*) de aquellas que afectan al propio sistema (*unauthorized access, unauthorized interception* y *unauthorized use of a computer),* así como las que provocan una interferencia en el curso del procesamiento de datos o en programas informáticos (*computer fraud - computer forgery*) o suponen meramente un acceso ilícito al sistema sin repercusión alguna en el funcionamiento del mismo (*unauthorized acces*).

c) ELEMENTOS DE LA PARTE OBJETIVA DEL TIPO

En tercer lugar, la Recomendación convierte en un elemento del tipo la infracción de medidas de seguridad, atribuyéndole un contenido muy amplio al entender como tales tanto las medidas de tipo mecánico como las de tipo lógico y que su infracción podía producirse o bien a través de su superación o bien mediante su desviación. No obstante, deja un amplio margen a los Estados para concretar este elemento, siempre con el límite de no exigir la superación del más alto grado de seguridad, caso en el que, considera, el delito devendría inaplicable[28].

En cuarto lugar, sustituye la expresión sin autorización (*without the authorization*) por la de sin derecho (*without right*) —cuya ajustada traducción al castellano sería, a mi juicio, más bien, la de ilícitamente— concepto que interpreta como más amplio y que asegura permite subsumir tanto las actuaciones que son ilícitas[29] porque el autor carece de la autorización del titular del sistema o excede los permisos concedidos por éste como aquellas que lo son porque resultan contrarias a la Ley[30].

3. PARTE SUBJETIVA DEL TIPO

La Recomendación no valora como necesaria la introducción de elementos específicos en el tipo subjetivo, aunque prevé para aquellos Estados que deseen castigar una modalidad más restringida de acceso ilícito la posibilidad de limitar el alcance de la aplicación del delito mediante el requerimiento de una intención subjetiva, tal y como, por cierto, hacía el Informe *Computer Related-Crime*[31].

---

[28] BEQUAI, 1990: 52.

[29] BEQUAI, 1990: 35.

[30] BEQUAI, 1990: 52.

[31] Igualmente, recomienda la previsión de un derecho premiante para aquellos supuestos en los que el accedente da inmediata noticia del acceso y de las vulnerabilidades del sistema a la víctima o a las autoridades, y tampoco especifica en este caso qué tipo de privilegio debe concedérsele al sujeto activo, es decir, si debe preverse un subtipo privilegiado, una semiexcusa absolutoria o una excusa absolutoria. BEQUAI, 1990: 53.

B) USO NO AUTORIZADO DE UN ORDENADOR

A diferencia del acceso ilícito a un sistema informático, el mero uso no autorizado de un ordenador aparece en la lista opcional como un comportamiento sin una extrema peligrosidad[32]. En este caso, la propuesta de incriminación contiene únicamente tres alternativas que difieren en atención al tipo de uso que efectúe del sistema informático el autor, ya que la mayor parte de los usos ilícitos dignos de sanción penal se hallan cubiertos por las figuras contempladas en la lista de mínimos[33].

1. BIEN JURÍDICO

Para la Recomendación, con esta concreta figura se protegen dos tipos de intereses: por un lado, los derechos económicos de la persona afectada y, por otra parte, la seguridad y el propio funcionamiento del sistema[34].

2. PARTE OBJETIVA Y SUBJETIVA DEL TIPO

Por lo que respecta a los elementos del tipo, propone castigar tanto los supuestos de ausencia de autorización como el ir más allá de la autorización concedida, prestando especial atención a aquellos casos en los que el uso no autorizado haya sido realizado un empleado[35]. Para restringir la conducta recomienda exigir una pérdida económica para el titular del sistema o la producción de un daño o la interrupción del funcionamiento de este último[36].

---

[32] Ello porque el sujeto activo del delito suelen ser empleados, personal administrativo, profesores de universidad y estudiantes. BEQUAI, 1990: 67.

[33] Consiste en: *El uso de un sistema informático o de una red de ordenadores ilícitamente, siempre que sea: realizado con conocimiento de la existencia de un importante riesgo de pérdida para el derecho de la persona titular del sistema o de causar un daño al sistema o a su funcionamiento; con la intención de causar una pérdida al titular del sistema o un daño al sistema o a su funcionamiento; causando pérdida a la persona autorizada a usar el sistema o daño al sistema o a su funcionamiento*. BEQUAI, 1990: 66.

[34] BEQUAI, 1990: 67.

[35] BEQUAI, 1990: 67.

[36] BEQUAI, 1990: 68.

IV. NACIONES UNIDAS: MANUAL *COMPUTER-RELATED CRIME*

La Recomendación 89 (9) —como cabe recordar, basada en el Informe *Computer-Related Crime* de 1986 de la Organización de Cooperación y Desarrollo Económico— conformó a partir de su aprobación un modelo a seguir para las distintas organizaciones de carácter supranacional a la hora de aprobar su respectiva normativa en materia de persecución y prevención de la delincuencia informática. En este sentido, el objetivo principal de cada una de estas iniciativas fue desde entonces el de potenciar el objetivo marcado en aquella: lograr una efectiva armonización penal en materia de delincuencia informática.

La primera organización en la que esto sucedió fue las Naciones Unidas, en el seno de la cual se aprobó el Manual *Computer-Related Crime*. A tal efecto, aunque la decisión de elaborar un manual en materia de prevención y control de la delincuencia informática fue adoptada en el *8th Congress on the Prevention of Crime and the treatment of Offenders*, celebrado en La Habana los días 27 de agosto a 7 de septiembre de 1990, a través de la Resolución 45/121, de 14 de diciembre de 1990, el debate sobre el contenido de la Recomendación 89 (9) y sobre el borrador del Manual no tuvo lugar, concretamente, hasta los días 5 a 8 de octubre de 1992 en el marco del Coloquio Preparatorio de Würzburg y 4 a 10 de septiembre 1994 durante el XV Congreso Internacional de Derecho Penal.

Teniendo en cuenta que dicho debate tuvo lugar en el transcurso del Congreso Internacional de Derecho penal y que en éste participaron los más preeminentes expertos de la época en la materia, considero conveniente analizar también, aunque brevemente, lo que se dijo en éste en relación con el acceso ilícito a un sistema informático. Por este motivo, el presente apartado se dividirá en dos partes: por un lado, el análisis de la conducta de acceso ilícito en el seno del Congreso Internacional de Derecho Penal y, por otro lado, el examen de la configuración de la conducta en el propio Manual.

A) CONGRESO INTERNACIONAL DE DERECHO PENAL

Como se ha indicado, los días 5 a 8 de octubre de 1992 tuvo lugar el Coloquio Preparatorio de Würzburg y los días 4 a 10 de septiembre 1994 el XV Congreso Internacional de Derecho Penal. Este Congreso, celebrado en Río de Janeiro y auspiciado por la Asociación Internacional de Derecho Penal, se estructuró en cuatro Secciones cada una de las cuáles se correspondía con un área del Derecho Penal de especial interés en el momento. De entre ellas, la segunda Sección fue específicamente dedicada a la delincuencia informática, debatiéndose, según se ha indicado, los ilícitos cuya incriminación había propuesto la Recomendación 89 (9)[37]. A continuación se presentan las consideraciones que en él se efectuaron respecto del acceso ilícito a un sistema informático y el uso no autorizado de un ordenador.

1. USO NO AUTORIZADO DE UN ORDENADOR

La tipificación del uso no autorizado de un ordenador se percibió como una cuestión especialmente problemática debido a la ausencia en los distintos ordenamientos jurídico-penales nacionales de tipos específicamente dirigidos a sancionar comportamientos constitutivos de hurto de uso[38]. Además, tampoco se consideró suficiente la potencialidad dañina de este tipo de usos —básicamente, el uso ilícito, principalmente personal, del ordenador de la empresa por parte de empleados de la misma— a los efectos de atribuir a la conducta la entidad suficiente como para garantizar una respuesta criminal conforme al principio de *ultima ratio*[39].

---

[37] Las Secciones en las que se dividió el Congreso fueron las siguientes: la primera de ellas fue dedicada a los delitos contra el medio ambiente, la segunda, a los delitos cometidos contra y por medio de la informática; la tercera, a los movimientos de reforma del Derecho Penal y los Derechos Humanos; y, la cuarta, a la regionalización del Derecho Penal Internacional y a la protección de los derechos del hombre en los procesos de cooperación internacional en materia penal.

[38] DURHAM, 1992: 100.

[39] DURHAM, 1992: 101.

2. ACCESO NO AUTORIZADO

Por otra parte, el acceso ilícito fue concebido como el fundamento fáctico de todos y cada uno de los hechos delictivos que pueden cometerse en relación con la informática[40]. Sin negar que existieron ciertas voces, minoritarias, en contra de proceder a su efectiva incriminación[41], lo cierto es que los expertos abogaron casi unánimemente por su tipificación, coincidiendo en su naturaleza de grave amenaza para los sistemas informáticos, principalmente por las siguientes razones: su naturaleza de barrera previa de todo un conjunto de ilícitos de extrema gravedad[42], la posibilidad de castigar únicamente la conducta de acceso en multitud de ocasiones[43], y los importantes perjuicios económicos que del acceso ilícito se pueden derivar para particulares y empresas[44].

---

[40] DURHAM, 1992: 98-99.

[41] Por ejemplo, el profesor SCHICK. KLEINKE y PURBACH, 1993: 695.

[42] DURHAM señaló que existen una multitud de razones por las cuales es necesario penalizarla, enumerando a este respecto las siguientes: en muchas ocasiones el mero acceso al sistema es la única huella que se podrá verificar la existencia de un delito cuya comisión permanecerá en la sombra; no es posible tipificar ciertos actos como delito si el mero acceso no lo es, principalmente, aquellas en las que lo que se castiga es la revelación pública de información sensible; el acceso en sí mismo es un delito que además contribuye a allanar el camino de más serias y dañosas conductas. DURHAM, 1992: 98-99.

[43] KLEINKE y PURBACH, 1993: 695.

[44] Especificó NILSON que el mero hecho de que un hacker intente tener acceso a un sistema informático habitualmente causa a las empresas importantes perjuicios económicos al tratar de averiguar exactamente cómo se ha producido el acceso. Continuó diciendo que los actos de acceso ilícito son peligrosos porque pueden producir en los sistemas errores, fallos, bloqueos o roturas, o porque los datos pueden ser destruidos por negligencia o los fallos de seguridad descubiertos o provocados pueden posteriormente ser usados para cometer ulteriores actividades delictivas, pues confiere acceso a datos que pueden comprometer seriamente la privacidad de la persona. Concluyó, por tanto, que esta conducta supone una gran amenaza para la sociedad que puede conducir o cubrir más seria criminalidad. En el mismo sentido, TIEDEMANN. NILSON, 1993: 695.

3. RECOMENDACIONES DE LA ASOCIACIÓN

Finalmente, la Asociación consideró recomendable la penalización tanto de los comportamientos previstos en la lista mínima como en la optativa[45]. La razón de lo anterior estribaba en que, en su opinión, el desarrollo de la informática reveló la existencia de lagunas en el Derecho penal tradicional consecuencia, principalmente, de la aparición de nuevos intereses dignos protección penal y del surgimiento de nuevas formas de agresión con un alto potencial lesivo a los bienes ya tutelados[46].

En cualquier caso, con el fin de realizar una correcta incriminación de tales conductas realizó dos sugerencias de extrema relevancia:

> a) Por una parte, sugirió que algunas definiciones, entre ellas el acceso no autorizado, fueran objeto de mayor concreción a la luz del progreso de la tecnología y de los cambios en la percepción de la delincuencia[47].
>
> b) Por otra parte, recomendó la criminalización de ciertos actos preparatorios dirigidos a proporcionar el acceso no autorizado, concretamente, el tráfico de claves (*passwords*) obtenidas ilegalmente y de otras informaciones o programas[48].

Ambas recomendaciones, pero muy especialmente la segunda, tendrán un reflejo en la normativa posterior, que recogerá una definición de acceso e introducirá una propuesta de punición de los actos preparatorios del acceso ilícito, tal y como se verá en apartados posteriores[49].

---

[45] AIDP, 1992: 84.

[46] AIDP, 1992: 84.

[47] AIDP, 1992: 84.

[48] AIDP, 1992: 684. AIDP, 1992: 84.

[49] Véase Apartado VI de este Capítulo.

B) MANUAL *COMPUTER-RELATED CRIME*

Durante el transcurso de la tercera y última parte del Congreso, el día 8 de octubre de 1992, tuvo lugar, tal y como se ha indicado, la reunión de expertos de las Naciones Unidas sobre la contribución de la organización a la persecución y prevención de la delincuencia informática. El objetivo principal de dicho encuentro fue la discusión del texto borrador del manual que la organización estaba redactando con el fin contribuir a la búsqueda de un consenso internacional sobre la criminalización nacional de las distintas conductas vinculadas a la informática de deseable punición.

Con el texto del Manual, los expertos consideraron oportuno dar un paso atrás en las propuestas de tipificación y regresar a la lista de recomendaciones del Informe *Computer-related Crime: Analysis of Legal Policy* de 1986. De este modo, decidieron proponer únicamente la incriminación de las conductas recogidas en la lista mínima de la Recomendación 89 (9), justificando esta idea en su mayor incidencia práctica y en la existencia de la mayor necesidad de su criminalización[50]. En consecuencia, siguiendo el texto del Informe, el Manual recomendó específicamente la tipificación del acceso ilícito, centrando, a diferencia de éste, la atención en el análisis de dos aspectos en concreto:

> **a) Objeto material del delito:** realizó un aportación sustancial por lo que respecta al objeto material del delito, resaltando la necesidad de entender englobados en el concepto de sistema informático no sólo el ordenador de sobremesa sino también cualquier dispositivo transportable, como los ordenadores portátiles, los teléfonos móviles y los restantes dispositivos con tecnología basada en microchips[51].

---

[50] Las conductas recogidas son: *fraud by computer manipulation*, *computer forgery*, *damage to or modifications of computer data programs, unauthorized access to computer systems and service* y *unauthorized reproduction of legally protected computer programs.*

[51] SECRETARIAT UNITED NATIONS, 1994: 14 párrafo 80.

b) Tipología del acceso: destacó la especial vulnerabilidad del sistema informático en dos supuestos específicos que, en mi opinión, permiten distinguir las distintas modalidades a través de las que puede tener lugar el acceso:

i) Accesos remoto: por un lado, hizo referencia a aquellos accesos llevados a cabo a través de las redes de comunicación, consiguiendo la superación de contraseñas de acceso al sistema, en los cuales, indicó, el hacker se aprovecha de la ventaja que suponen las laxas medidas de seguridad[52].

ii) Accesos físicos: por otro lado, hace hincapié en la posibilidad de que el acceso tenga lugar en relación con aquellos sistemas empleados por diversas personas con contraseñas comunes o sistemas en los que las contraseñas maestras se pueden encontrar en el propio sistema[53].

C) ETAPA POSTERIOR A LA ELABORACIÓN DEL MANUAL

Sobre la base de la Recomendación (89) 9 y del Manual, Naciones Unidas siguió y, de hecho, continúa a día de hoy trabajando en el análisis y estudio de la delincuencia informática[54]. Por lo que respecta al acceso ilícito, debe destacarse el *Background paper for workshop on crimes related to the computer network* del *10th United Nations Congress on the Prevention of Crime and the treatment of Offenders* que analiza cómo se han traducido legislativamente en los distintos países las recomendaciones de la Asociación[55].

---

[52] SECRETARIAT UNITED NATIONS, 1994: 14 párrafo 74.

[53] La contraseña no es, para los redactores del manual, un instrumento eficaz contra el acceso no autorizado, ya que la comunidad internacional criminal de *hackers* usa boletines electrónicos para comunicar las infiltraciones en los sistemas y los métodos utilizados para ello, hecho que facilita la multiplicación de las infiltraciones en el sistema por todo el mundo. SECRETARIAT UNITED NATIONS, 1994: 14 párrafos 75-76; 15 párrafos 79-80.

[54] La décima del año 2000, la undécima del 2005 y la duodécima del 2010.

[55] SECRETARIAT UNITED NATIONS, 1990b: 6 párrafo 16.

V. PLAN DE ACCIÓN DEL G8

También el G-8 se hizo eco de la iniciativa llevada a cabo por las distintas organizaciones en materia de delincuencia informática y decidió acoger como propio el propósito armonizador pretendido por el Informe, la Recomendación 89 (9) y el Manual. Así, los días 9 y 10 de diciembre de 1996 adoptó en París las *Senior Experts Group Recommendations To Combat Transnational Organized Crime Efficiently*, en cuyo punto 10.9 estableció como uno de los objetivos principales del Grupo revisar la normativa aprobada por las distintas organizaciones internacionales sobre delincuencia informática, garantizar la criminalización de las conductas merecedoras de sanción penal en los distintos países que lo conformaban y arbitrar los mecanismos necesarios para lograr una efectiva aplicación práctica de las disposiciones aprobadas mediante la aproximación de todo lo relativo a la jurisdicción, las facultades de aplicación, la investigación, la formación, la prevención del delito y la cooperación internacional en la materia[56].

A) *SUBGROUP ON HIGH-TECH CRIME*

A los efectos de cumplir los tres fines marcados, en 1997 el G-8 creó el *Subgroup on High-Tech Crime*, también llamado *Lyon-Group*, el cual a partir de entonces tendría como función el establecimiento de una adecuada coordinación entre los países participantes para prevenir, investigar y perseguir los delitos relacionados con los sistemas informáticos, las redes de comunicaciones y los demás ilícitos derivados de las nuevas tecnologías.

---

[56] 10.9 *States should review their laws in order to ensure that abuses of modern technology that are deserving of criminal sanctions are criminalized and that problems with respect to jurisdiction, enforcement powers, investigation, training, crime prevention and international cooperation in respect of such abuses are effectively addressed. Liaison between law enforcement and prosecution personnel of different States should be improved, including the sharing of experience in addressing these problems. States should promote study in this area and negotiate arrangements and agreements to address the problem of technological crime and investigation.* SENIOR EXPERTS GROUP ONTRANSNATIONAL ORGANIZED CRIME G7 + RUSSIA, 1996: punto 10.9.

B) DERECHO SUSTANTIVO: *TEN PRINCIPLES AND ACTION PLAN IN THE COMBAT AGAINST COMPUTER CRIME*

En el plano sustantivo, sobre la base del trabajo del Subgrupo, el Grupo adoptó los *Ten Principles and Action Plan in the combat against computer crime* en la reunión de Ministros de Justicia y del Interior celebrada los días 16 a 18 de abril de 1997. Estos documentos tuvieron un contenido más preciso que las Recomendaciones de París de 1996, siendo, respectivamente, el principio 4[57] y el punto 3[58] del Plan de Acción donde se dejó patente la necesidad de proteger la confidencialidad, integridad y disponibilidad de los datos y sistemas informáticos frente a su abuso y menoscabo.

C) DERECHO PROCESAL: *BIRMINGHAM SUBMIT Y SIX PRINCIPLES ON TRANSBORDER ACCESS TO STORED COMPUTER DATA*

En el ámbito procesal, fue en la cumbre de Jefes de Estado celebrada en Birmingham los días 15 a 17 de mayo de 1998 donde, tras resaltar el carácter transfronterizo de éste tipo de criminalidad, se adoptó *Birmingham submit*[59], a través del cual se señalaron los puntos sobre los que serían necesario alcanzar un acuerdo[60]:

---

[57] *IV. Legal systems must protect the confidentiality, integrity, and availability of data and systems from unauthorized impairment and ensure that serious abuse is penalized.* SUBGROUP ON HICH-TECH CRIME G7 + RUSSIA, 1997:.

[58] 3. *Review our legal systems to ensure that they appropriately criminalize abuses of telecommunications and computer systems and promote the investigation of high-tech crimes.* SUBGROUP ON HICH-TECH CRIME G7 + RUSSIA, 1997: 1.

[59] *18. Globalization has been accompanied by a dramatic increase in transnational crime. This takes many forms, including trafficking in drugs and weapons; smuggling of human beings; the abuse of new technologies to steal, defraud and evade the law; and the laundering of the proceeds of crime.* HEADS OF STATE OF G8 AND THE PRESIDENT OF THE EUROPEAN COMMISSION, 1998: punto 18..

[60] *21.2 We agree to implement rapidly the ten principles and ten point action plan agreed by our Ministers on high tech crime. We call for close cooperation with industry to reach agreement on a legal framework for obtaining, presenting and preserving electronic data as evidence, while maintaining appropriate privacy protection, and agreements on sharing evidence of those crimes with international partners. This will help us combat a wide range of crime, including abuse of the internet and other new technologies.* HEADS OF STATE OF G8 AND THE PRESIDENT OF THE EUROPEAN COMMISSION, 1998: 1 punto 21.2..

a) La obtención, presentación y preservación de datos electrónicos como prueba.

b) El mantenimiento de la protección de la privacidad.

c) El intercambio de pruebas de esos delitos.

Como concreción de estas tres ideas, fueron adoptados en el seno de la *Ministerial Conference of the G-8 Countries on Combating Transnational Organized Crime,* celebrada en Moscú los días 19 y 20 de 1999, un conjunto de seis principios sobre acceso transfronterizo a datos informáticos para viabilizar la preservación y el acceso sin necesidad de asistencia legal a los datos almacenados en un sistema informático situado en un país extranjero, la asistencia jurídica mutua y la cooperación judicial[61].

D) DE LA DELINCUENCIA INFORMÁTICA AL CIBERCRIMEN: *OKINAWA SUBMIT*

El carácter transnacional de la delincuencia informática hizo que paulatinamente la atención se fijara en un aspecto muy concreto de ésta: Internet, el medio mediante el cual la mayor parte de estos comportamientos delictivos tenían lugar. Internet se fue percibiendo cada vez más como el aspecto más globalizador y a la vez más peligroso de la nueva sociedad informatizada. En este sentido, al combate de la llamada criminalidad cibernética se dirigieron a partir de este momento los esfuerzos armonizadores en el ámbito internacional. Concretamente, en el marco del G-8 se adoptó el *Okinawa Submit* en la reunión de Jefes de Estado celebrada los días 21 a 23 de julio del año 2000, que centró el nuevo foco de atención en la seguridad y la confianza en la sociedad de la información mundial[62].

---

[61] G-8 MINISTERIAL MEETINGS ON CRIME, 1999: 1 y ss.

[62] *44. We must take a concerted approach to high-tech crime, such as cyber-crime, which could seriously threaten security and confidence in the global information society. Our approach is set out in the Okinawa Charter on Global Information Society.* HEADS OF STATE OF G8 AND THE PRESIDENT OF THE EUROPEAN COMMISSION, 2000: párrafo 44.

VI. CONSEJO DE EUROPA: CONVENIO SOBRE CIBERCRIMEN

En la década de los 90 ya existía cierto grado de aproximación entre las distintas legislaciones nacionales en materia de delincuencia informática y cibercrimen, pero el objetivo de alcanzar una política penal uniforme todavía estaba lejos. Subsistían, pues, discrepancias considerables entre los ordenamientos jurídico-penales de los distintos países[63].

Fueron varios los Informes que elaboraron las distintas organizaciones al respecto[64], señalando como motivo de lo anterior el carácter meramente recomendatorio de las normas aprobadas. Ello, de hecho, fue especialmente resaltado por el profesor KASPERSEN en su *Informe sobre la Aplicación de la Recomendación (89) 9* de 1997: *debería recurrirse a un instrumento jurídico que implicara mayor compromiso que una recomendación, tal como un convenio. Dicho convenio no solo debería tener un contenido de Derecho penal sustantivo, sino también cuestiones de Derecho procesal penal, así como procedimientos y acuerdos en materia de Derecho penal internacional*[65].

---

[63] Concretamente por lo que se refería al acceso ilícito, mientras que algunos países sí castigaban el acceso al sistema (Dinamarca, Francia, Suecia o Estados Unidos), en otros, (como Canadá, República Federal de Alemania, República Democrática Alemana o Noruega) la protección se ofrecía únicamente a los datos informáticos (especialmente personales).

[64] El Informe interno del Secretariado de las Naciones Unidas para el *9th United Nations Congress on the Prevention of Crime and the treatment of Offenders*, celebrado en El Cairo, del 29 de abril al 8 de mayo de 1995, —sobre cooperación internacional y asistencia técnica práctica para el fortalecimiento de las reglas del Derecho en el marco del programa de promoción por parte de las Naciones Unidas de la prevención del delito y la justicia criminal—, en la cual se analizaban las experiencias nacionales y la cooperación internacional relativas a la acción sobre delincuencia económica y organizada nacional y transnacional y el rol del Derecho penal en la protección del medio ambiente, pone de manifiesto que en materia de delincuencia informática solo quince Estados (entre los que no incluye Italia) informan acerca de haber aprobado regulación penal en la materia (Australia, Bahrein, Chile, Colombia, Costa Rica, Dinamarca, Francia, Alemania, Grecia, Hungría, Japón, Noruega, Portugal, Singapur, Suiza), de los cuales únicamente tres hacen referencia expresa a previsiones específicas que, por otra parte, refieren particularmente al fraude. SECRETARIAT UNITED NATIONS, 1990a: 12 párrafos 39-40.

[65] KASPERSEN, 1997: 106.

Acogiendo la propuesta del profesor, el Comité Europeo para los Problemas Criminales del Consejo de Europa creó el Comité de Expertos en Delincuencia del Ciberespacio[66], atribuyéndole como único cometido la elaboración de un instrumento de carácter vinculante capaz de asegurar una efectiva armonización de los ordenamientos jurídico-penales nacionales de los países parte del Consejo de Europa en la lucha contra dicha forma de criminalidad.

Entre 1997 y el año 2000 el Comité celebró diez sesiones Plenarias y su Grupo de Redacción, de composición abierta, organizó otras quince ordinarias en las que se debatieron cada una de las conductas recogidas en los textos analizados en los apartados precedentes, prestando una especial atención a la Recomendación (89) 9, la cual constituyó el modelo a seguir por el Comité[67]. Transcurridos cuatro años de la creación del Comité, en la segunda parte de la sesión de abril de 2001, el Pleno del Comité adoptó finalmente el texto del Proyecto de Convenio sobre Cibercrimen el 23 de noviembre de 2001, que se abriría a la firma en una ceremonia celebrada en Budapest el 23 de noviembre de 2001.

El Convenio sobre Cibercrimen fue la primera norma vinculante dirigida a la consecución (no ya a la mera potenciación) del propósito que habían tenido todas y cada una de las iniciativas internacionales adoptadas desde hacía tres décadas: lograr la efectiva armonización penal de las distintas legislaciones nacionales en materia informática.

---

[66] Creado por Decición CM/Del/Dec(97)583, del Consejo de Ministros del Consejo de Europa, adoptada en la reunión nº 583 del 4 de febrero de 1997.

[67] El mandato específico del Comité consiste, desde una perspectiva sustantiva, en examinar a la luz de la Recomendación (89) 9 las cuestiones de Derecho penal vinculadas a la tecnología de la información y, más concretamente: los delitos cometidos en el ciberespacio, en particular mediante el uso de las redes de telecomunicaciones como Internet, y aquellas otras en las que es necesario ofrecer un enfoque común a fin de lograr la cooperación internacional tales como definiciones, sanciones y la responsabilidad de las personas activas en el ciberespacio, incluidos los proveedores de servicios de Internet. Para más información, véase Explanatory Report to the Convention on Cybercrime, accesible en http://conventions.coe.int/treaty/en/reports/html/185.htm.

La importancia del Convenio es extrema por tres motivos:

a) En primer lugar, debido a su **naturaleza**. Se trata de la primera norma de carácter vinculante aprobada en materia de delincuencia informática y, en este sentido, fue la disposición que, como ya había avanzado KASPERSEN, dio el impulso definitivo para la consolidación de una verdadera uniformidad de las regulaciones nacionales en relación con el fenómeno informático.

b) En segundo lugar, por su **ámbito de protección**. No se centra únicamente en proteger los propios elementos informáticos, sino que tiene en cuenta el nuevo foco generalizado de delincuencia vinculada a Internet. En este sentido, sus redactores supieron entender como había surgido un nuevo espacio común, el ciberespacio, que facilita multitud de posibilidades para la comisión de delitos contra la integridad, disponibilidad y la confidencialidad de los sistemas informáticos y de las redes de telecomunicaciones, así como contra el uso de esas redes o sus servicios para cometer delitos tradicionales.

c) En tercer lugar, el último aspecto destacable del Convenio es la **inclusión de disposiciones procesales**. Tiene en cuenta el carácter transfronterizo de esta forma de criminalidad y arbitra distintos mecanismos de cooperación internacional para viabilizar la lucha contra la misma[68].

---

[68] En este sentido, se aduce como motivo principal que el rápido desarrollo de la tecnología de la información influye directamente sobre todos los sectores de la sociedad moderna y la integración de los sistemas de telecomunicaciones y de información, que se ha visto potenciada por la aparición de las redes y las autopistas de la información como Internet, posibilita el almacenamiento y la transmisión de todo tipo de comunicaciones sin tener en cuenta la distancia ya que prácticamente todas las personas pueden tener acceso a cualquier servicio de información electrónica, sin importar en qué lugar del mundo se encuentre. COUNCIL OF EUROPE, 2001: 11 párrafo 34. SECRETARIAT UNITED NATIONS, 1990b: 3 párrafo 3. Decisión CDPC/103/211196 del Comité Europeo para los Problemas Criminales del Consejo de Europa.

A) ESTRUCTURA Y CONTENIDO

Por lo que se refiere a su estructura, el Convenio cuenta con un Preámbulo y cuatro Títulos: Terminología; Medidas a adoptar en el ámbito nacional, (subdividido, a su vez, en dos Secciones: Derecho penal material y Derecho procesal penal); Cooperación internacional; y Cláusulas finales. Así pues, incorpora tanto normas de naturaleza penal como procesal, aunando en un mismo texto todos los aspectos necesarios para la consecución no solo de una armonización penal nacional sino también de la cooperación internacional que permite hacerla viable. Este hecho marca un hito fundamental en relación con la normativa internacional aprobada hasta el momento, cuyo desarrollo se había llevado a cabo de forma sesgada en el seno de las distintas organizaciones internacionales. Efectivamente, cada uno de estos ámbitos había sido objeto de regulación por separado y a través de normas en la mayor parte de ocasiones desconectadas temporalmente, produciéndose además de una notable fragmentación y dispersión normativa, una absoluta disgregación de la implementación nacional de los distintos mecanismos que los Estados debían implementar para hacer frente a un mismo fenómeno[69].

En cuanto a contenido, el Convenio mantuvo en general las directrices desarrolladas por la Recomendación (89) 9 del Consejo de Europa, de la que conservó en su mayor parte su redacción por lo que al Derecho penal material se refiere. No obstante, introdujo importantes novedades que contribuyeron a una mejor implementación de sus disposiciones. Entre ellas deben resaltarse ahora dos:

---

[69] Ello se evidenció claramente en el Preámbulo del Convenio, donde se especificaron los tres fines que se perseguía a través de su adopción, a saber, la armonización del Derecho penal sustantivo en materia informática, la creación un marco común que posibilitase la investigación y el procesamiento por dichos delitos y el establecimiento de un régimen rápido y eficaz de cooperación internacional. Véase Preámbulo del Convenio y COUNCIL OF EUROPE, 2001: 6 párrafo 16.

a) El Convenio dedica un Capítulo I, rubricado Terminología y que solo comprende un precepto, el artículo 1, a establecer una serie de definiciones comunes sobre los términos técnicos más importantes utilizados a lo largo de todo su articulado. Se trata de una diferencia sustancial respecto de los documentos anteriores, que habían optado expresamente por no ofrecer una definición de los conceptos técnicos en ellos utilizados para mantener su neutralidad[70]. Quizá por esta razón el propio Convenio hace alusión específicamente a este aspecto[71].

b) En la Sección I del Capítulo II incorpora las disposiciones relativas al Derecho penal material y que se corresponden con las disposiciones de la lista mínima de la Recomendación[72]. En ella se prevén tanto las cuestiones sobre la tipificación armonizada de las conductas relativas al medio informático –nueve infracciones[73], agrupadas en cuatro categorías[74]– como también algunas referentes a ciertos aspectos adyacentes, tales como la forma de comisión del delito, la responsabilidad y las sanciones.

---

[70] Cabe recordar que el Informe Final a la Recomendación explica como, a pesar de que originariamente los miembros del Comité tenían la intención de elaborar un glosario de términos común y consensuado como apéndice al Informe para que fuera usado a los efectos de interpretar la Recomendación, por múltiples razones, entre ellas la de más peso el deseo mantener la neutralidad, decidieron finalmente no adoptar definiciones con carácter formal e, incluso, mantenerse al margen de ofrecer una noción jurídica de delito informático. BEQUAI, 1990: 35-36.

[71] COUNCIL OF EUROPE, 2001: 11 párrafo 36. Al respecto, véase también COUNCIL OF EUROPE, 2012b: 1 y ss.

[72] Elimina las conductas de la lista opcional.

[73] Acceso ilícito, interceptación ilícita, ataques a la integridad de los datos, ataques a la integridad del sistema, abuso de dispositivos, falsificación informática, fraude informático, delitos relacionados con la pornografía infantil y delitos relacionados con infracciones de la propiedad intelectual y de los derechos conexos.

[74] Delitos contra la confidencialidad, integridad y disponibilidad de datos o sistemas informáticos; Delitos asociados a la informática; Delitos relacionados con el contenido; y los Delitos relacionados con infracciones de la propiedad intelectual y los derechos afines.

B) EL DELITO DE ACCESO ILÍCITO

El acceso ilícito aparece recogido en el artículo 2 del Título I de la Sección 1 del Capítulo II del Convenio, dedicado a los delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos[75]. En concreto, es el primer delito cuya incriminación propone: *el acceso doloso e ilícito a la totalidad o a una parte de un sistema informático*[76], permitiendo a a los Estados añadir algunas exigencias de carácter facultativo para configurar la infracción penal: *requerir que el hecho sea cometido infringiendo medidas de seguridad o con la finalidad de obtener datos informáticos u otra finalidad deshonesta o, en relación con los sistemas informáticos, que se encuentren conectados a otros sistemas informáticos*[77]. En cuanto a la configuración específica de los elementos del tipo, puede destacarse lo siguiente:

1. BIEN JURÍDICO PROTEGIDO

El acceso ilícito es concebido como el delito básico contra las amenazas y ataques a la seguridad[78] y el medio a través del cual brindar protección al sistema de forma adicional a las posibles medidas de seguridad que el usuario tenga instaladas en el sistema[79]. Su incriminación responde, de este modo, a la necesidad de proteger a los usuarios legítimos de los sistemas frente a intromisiones que puedan conducir a la comisión de ilícitos con un mayor contenido de injusto[80].

---

[75] COUNCIL OF EUROPE, 2001: 11 párrafo 35.

[76] *Article 2 – Illegal access. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the access to the whole or any part of a computer system without right.*

[77] *A Party may require that the offence be committed by infringing security measures, with the intent of obtaining computer data or other dishonest intent, or in relation to a computer system that is connected to another computer system.*

[78] COUNCIL OF EUROPE, 2001: 13 párrafo 44.

[79] COUNCIL OF EUROPE, 2001: 13-14 párrafos 44-45.

[80] Acceso a datos confidenciales, acceso a secretos, fraudes o falsificación informática. COUNCIL OF EUROPE, 2001: 13 párrafo 44.

2. ELEMENTOS DEL TIPO

Por lo que se refiere a la tipicidad, cabe señalar que ésta se ve reducida a la mínima expresión, proponiéndose castigar únicamente el acceso doloso a la totalidad o a una parte del sistema informático, sin que ningún otro elemento sea considerado determinante para la realización del tipo. Aun así, el Convenio prevé la posibilidad de añadir dos elementos restrictivos del tipo objetivo: que el hecho sea cometido infringiendo medidas de seguridad o que el sistema informático se encuentre en red; y/o un elemento subjetivo del injusto: la finalidad de obtener datos informáticos u otra finalidad deshonesta. Sin embargo, se trata únicamente posibilidades a tener en cuenta por los legisladores nacionales, que pueden o no incluirlos al efectuar la transposición de las disposiciones del Convenio en sus respectivos Derechos internos[81].

Con tal redacción, el Convenio retomó en gran medida la redacción ofrecida por el Informe *Computer-related crime: Analysis of legal policy*, en el cual, aunque la conducta era la misma, se preveía la inclusión alternativa de alguno de los dos siguientes elementos: o bien la infracción de medidas de seguridad, o bien que la conducta del sujeto viniera informada por cualquier finalidad deshonesta, elemento cuya inespecificidad suponía, en mi opinión, más que la adición de un elemento subjetivo del injusto, la limitación de la conducta típica únicamente a la modalidad doloso-directa[82].

---

[81] Con ello se pretendió brindar a los Gobiernos y Parlamentos flexibilidad para poder adaptar su política criminal en la materia en atención a las diferentes percepciones existentes en cada país respecto de la peligrosidad del comportamiento involucrado o de la necesidad de usar el Derecho penal como medio de control social. Así pues, por una parte les permite excluir la incriminación de aquellas conductas que consideren de escasa relevancia en su ordenamiento jurídico y, por otra, ciertos artículos permiten añadir elementos a efectos de restringir el tipo. Éste es el caso específico del acceso ilícito que, como puede verse permite añadir, como se ve, el requerimiento de que *el hecho sea cometido infringiendo medidas de seguridad o con la finalidad de obtener datos informáticos u otra finalidad deshonesta o, en relación con los sistemas informáticos, que se encuentren conectados a otros sistemas informáticos*. COUNCIL OF EUROPE, 2001: 12 párrafos 37 y 40.

[82] Véase Apartado II de este Capítulo.

Lo anterior marca una clara diferencia entre el Convenio y la Recomendación (89) 9 del Consejo de Europa, ya que en ésta la vulneración de las medidas de seguridad conformaba un elemento integrante del tipo objetivo y no un elemento facultativo, lo que suponía una notable restricción de su ámbito aplicativo en comparación con la norma que en este momento se aprobaba[83].

A continuación se estudiarán con más detalle cada uno de los elementos que componen la tipicidad objetiva y subjetiva de la conducta:

a) PARTE OBJETIVA DEL TIPO

Por lo que respecta a la parte objetiva, como se ha indicado, el Convenio otorga la mayor libertad posible a los Estados en la configuración de la tipo, debiéndose destacar al respecto los siguientes aspectos:

i) CONDUCTA

El Convenio conserva desglosadas las conductas de acceso e interceptación como ya hacía la Recomendación (89) 9 del Consejo de Europa, recogiéndolas de forma consecutiva en los artículos 2 y 3 respectivamente. Mientras el acceso se predica respecto del propio sistema –la protección de los intereses de las personas en la utilización, la operación y el control de sus sistemas informáticos sin interrupciones ni restricciones–[84], la interceptación va referida a los datos informáticos contenidos en él o destinados por o hacia él, con el objetivo último de proteger la privacidad[85]. A tal efecto, el acceso es definido como la mera intromisión no autorizada, es decir, la "piratería" (*hacking*), el "sabotaje" (*cracking*) o "la intrusión en el ordenador" (*computer trespass*)[86].

---

[83] Véase apartado III de este Capítulo.

[84] COUNCIL OF EUROPE, 2001: 13 párrafo 44.

[85] COUNCIL OF EUROPE, 2001: 15 párrafos 51-52.

[86] COUNCIL OF EUROPE, 2001: 13 párrafo 44.

ii) OBJETO MATERIAL DEL DELITO

Como he apuntado anteriormente[87], la diferencia sustancial entre el Convenio y los textos del Informe y de la Recomendación radica en que éste dedica su Capítulo I, rubricado Terminología, y que solo comprende un precepto, el artículo 1, a establecer una serie de definiciones comunes sobre los términos técnicos que se utilizan a lo largo de todo el texto[88]. Así, se prevén el concepto de sistema informático, de datos informáticos, de proveedor de servicios y de datos relativos al tráfico.

Para el estudio del delito de acceso ilícito, será necesario ahondar únicamente en los conceptos de sistema informático y datos informáticos, además del de datos relativos al tráfico (aunque éste simplemente para deslindarlo del anterior), el primero porque el sistema informático constituye el objeto material del delito de acceso ilícito en el Convenio y, con las salvedades que más adelante se expondrán, en el artículo 197.1 *bis* del Código penal[89], el segundo porque los datos informáticos fueron el objeto material del delito de acceso ilícito según la redacción del tipo vigente en España desde el año 2010 al 2015, introducida por la Ley Orgánica 5/2010, de 22 de junio, en el artículo 197.3 del Código penal[90]. Ello permitirá, pues, más adelante analizar la compatibilidad de los términos previstos en el Convenio con los recogidos en el artículo 197.1 *bis*.

---

[87] Véase apartado A) de este punto.

[88] En la línea de permitir a los Estados la mayor flexibilidad posible en la transposición de las disposiciones del Convenio, éste refirió el carácter puramente orientativo de las distintas nociones recogidas en él. De este modo, los Estados no estaban obligados a introducirlas de forma literal sino simplemente a respetar la coherencia y finalidad de los principios en los que se inspiraron. Esta voluntad dispositiva del Convenio respecto de los Estados se manifestó específicamente en el término datos de tráfico, en relación con el cual dejó un margen a cada país para definir esta categoría de acuerdo con las especiales necesidades de su ordenamiento jurídico, previendo cierto grado de diferenciación —no muy amplio porque la importancia de los datos de tráfico se despliega sobre todo en el ámbito procesal como sustento de alguna prueba informática — respecto de su protección legal. En general, COUNCIL OF EUROPE, 2001: 7 párrafo 22. Respecto de los datos de tráfico COUNCIL OF EUROPE, 2001: 10 párrafo 31.

[89] Véase Sección 2ª del Capítulo V.

[90] Véase Sección 1ª del Capítulo V.

aa) SISTEMA INFORMATICO

De acuerdo con el artículo 1 a) del Convenio, el sistema informático es concebido como *todo dispositivo aislado o conjunto de dispositivos interconectados o unidos entre sí que aseguran, al ejecutar un programa, el tratamiento automatizado de datos informáticos*[91]. Conforme a la definición transcrita, dos son las características básicas del sistema informático: estar compuesto por un dispositivo o conjunto de dispositivos de carácter físico (*hardware*) interconectados entre sí (*software*) con la función de tratamiento automatizado de datos (entrada, procesamiento y salida de datos), siendo tales dispositivos susceptibles de trabajar de forma independiente o en conexión de red con otros dispositivos similares[92]. A continuación, se presentará con más detalle el desarrollo que efectúa el Convenio de cada uno de estos elementos:

aaa) SISTEMA INFORMÁTICO COMO CONJUNTO DE DISPOSITIVOS FÍSICOS: EL HARDWARE

El primer elemento del que se compone el sistema informático es de uno o varios dispositivos que reciben el nombre de hardware. Tales dispositivos pueden ser de dos tipos: interno (*input*) o externo (*output*)[93]. El hardware interno básico es el procesador o unidad de procesamiento central, que permite el funcionamiento de todo el sistema, mientras que el externo, también llamado dispositivos periféricos, realiza únicamente funciones específicas asignadas al sistema interactuando con la unidad de procesamiento[94]. Son dispositivos periféricos la impresora, la pantalla, el lector de CD o DVD y, en general, cualquier otro dispositivo de almacenamiento de datos[95].

---

91 *"computer system" means any device or a group of interconnected or related devices, one or more of which, pursuant to a program, performs automatic processing of data.*

92 COUNCIL OF EUROPE, 2001: 7 párrafo 23.

93 COUNCIL OF EUROPE, 2001: 7 párrafo 23.

94 COUNCIL OF EUROPE, 2001: 7 párrafo 23.

95 COUNCIL OF EUROPE, 2001: 7 párrafo 23.

bbb) INTERCONEXIÓN DEL HARDWARE PARA EL TRATAMIENTO AUTOMATIZADO DE DATOS: EL SOFTWARE

El segundo elemento que integra el sistema informático es el software, esto es, *a grosso modo*, el conjunto de programas que posibilitan el funcionamiento del sistema. El software, por tanto, tiene como función viabilizar la ejecución de las funciones del hardware para el tratamiento automatizado sin intervención humana de los datos, hecho que tiene lugar a través de la ejecución de múltiples programas informáticos[96]. El concepto de programa informático, que no viene recogido en la Convención, sí lo es en el Informe anejo a la misma, que lo define como *el conjunto de instrucciones que pueden ser ejecutadas por el equipo para alcanzar el resultado deseado*[97].

ccc) SUSCEPTIBILIDAD DE INTERCONEXIÓN

La tercera y última de las características que el Convenio predica del sistema es su susceptibilidad de trabajo independiente o en conexión a otros sistemas informáticos como nodos o como instrumento para brindar asistencia en la comunicación entre los distintos sistemas interconectados[98]. La conexión a la que se hace referencia recibe el nombre de red y su función principal es el intercambio de datos[99]. Una red puede ser terrestre (inalámbricas o por cable), inalámbrica (radioeléctricas, infrarrojas o satelitales), o de ambos tipos, y, además, puede estar limitada geográficamente a un área pequeña (redes de área local) o puede abarcar un área extensa (redes de área extensa)[100]. También existen redes interconectadas que utilizan protocolos comunes como, por ejemplo, sucede con Internet[101].

---

[96] COUNCIL OF EUROPE, 2001: 7 párrafo 23.

[97] COUNCIL OF EUROPE, 2001: 7 párrafo 23.

[98] COUNCIL OF EUROPE, 2001: 8 párrafo 24.

[99] COUNCIL OF EUROPE, 2001: 8 párrafo 24.

[100] COUNCIL OF EUROPE, 2001: 8 párrafo 24.

[101] COUNCIL OF EUROPE, 2001: 8 párrafo 24.

ddd) EXTENSIÓN DEL CONCEPTO DE SISTEMA INFORMÁTICO

Aunque en principio cualquier dispositivo que ostente ambas características debe haber ser considerado sistema informático, generalmente este concepto se ha asimilado al de ordenador. Sin embargo, el surgimiento de nuevos instrumentos electrónicos de idéntica composición y funcionalidad que los anteriormente mencionados hizo necesaria una reinterpretación del concepto de sistema informático. Con este objeto, el octavo Plenario del Comité de la Convención de Cibercrimen, celebrado los días 20 y 21 de marzo de 2006, a la luz del desarrollo de una nueva generación de dispositivos informáticos que van más allá del mero ordenador de escritorio, ha extendido el concepto de sistema informático a los *smartphones*, las PDAs, las *tablets* y los mecanismos similares de procesamiento de datos[102].

bb) DATOS INFORMÁTICOS Y DATOS DE TRÁFICO

La letra b) del artículo 1 define datos informáticos como *toda representación de hechos, informaciones o conceptos expresados bajo una forma tratable informáticamente, incluido el programa destinado a hacer que un sistema informático ejecute su función*[103], mientras que la letra d) precisa la de datos de tráfico: *todos los datos relativos a una comunicación realizada por medio de un sistema informático, generados por este último en tanto que elemento de la cadena de comunicación, y que indiquen el origen, el destino, la ruta, la hora, la fecha, el tamaño y la duración de la comunicación o el tipo de servicio subyacente*[104]. Aunque ambos son datos, parece tratarse de dos categorías distintas de éstos, razón por la que se hace imprescindible una explicación al respecto:

---

[102] COUNCIL OF EUROPE, 2012a: 1 y ss..

[103] *"computer data" means any representation of facts, information or concepts in a form suitable for processing in a computer system, including a program suitable to cause a computer system to perform a function.*

[104] *"traffic data" means any computer data relating to a communication by means of a computer system, generated by a computer system that formed a part in the chain of communication, indicating the communication's origin, destination, route, time, date, size, duration, or type of underlying service.*

aaa) DATOS INFORMATICOS

El concepto de datos informáticos incluido en el Convenio ess reflejo directo de la noción de datos de la Organización Internacional de Normalización (ISO), que definió como tales todos aquellos con un fin directo de tratamiento automatizado de datos[105]. Ello supone considerar datos informáticos tanto los contenidos en formato electrónico en el sistema como todos los procesados por cualquier otro medio siempre sean susceptibles de tratamiento informático[106].

bbb) DATOS DE TRÁFICO

Los datos de tráfico son una categoría de datos informáticos sujeta a un régimen jurídico específico[107]. Concretamente, son aquellos datos que se generan como efecto auxiliar de la cadena de comunicación entre distintos sistemas informáticos y que tienen la finalidad de conducir la comunicación desde su origen hasta su destino[108], permitiendo rastrearla, averiguar la ruta que ha seguido, o identificar el sistema informático emisor y el receptor[109]. El Convenio enumera de forma exhaustiva cuáles son: el origen de una comunicación, su destino, la ruta, la hora (GMT), la fecha, el tamaño, la duración y el tipo de servicio subyacente[110].

---

[105] COUNCIL OF EUROPE, 2001: 8 párrafo 25.

[106] COUNCIL OF EUROPE, 2001: 8 párrafo 25.

[107] La obtención de estos datos es considerada menos intrusiva que la obtención de datos de la comunicación en la medida en que no se revela el contenido de la comunicación, que es la parte más sensible de la misma. COUNCIL OF EUROPE, 2001: 9 párrafo 29.

[108] COUNCIL OF EUROPE, 2001: 9 párrafo 28.

[109] COUNCIL OF EUROPE, 2001: 9 párrafo 29.

[110] Según explica el Informe, el *origen* de la comunicación hace referencia a un número de teléfono, dirección de Protocolo de Internet (IP), o a una identificación similar de una instalación de comunicaciones a la que un proveedor de servicios presta sus servicios; mientras que el *destino* de la comunicación alude a una indicación comparable de una instalación de comunicaciones a las que se transmiten las comunicaciones. La expresión *tipo de servicio* subyacente alude al tipo de servicio que está siendo utilizado en la red, el cual puede ser, a título de ejemplo, una transferencia de archivos, un correo electrónico o el envío de mensajes instantáneos. COUNCIL OF EUROPE, 2001: 9 párrafo 30. COUNCIL OF EUROPE, 2001: 10 párrafo 30.

iii) OTROS ELEMENTOS DEL TIPO OBJETIVO: LA EXPRESIÓN *WITHOUT RIGHT* Y LA VULNERACIÓN DE MEDIDAS DE SEGURIDAD

Aunque como se ha indicado el Convenio reduce la conducta básica a la mínima expresión por lo que se refiere a la parte objetiva del tipo, dos aspectos más deben comentarse además de la acción y del objeto material del delito. Son los siguientes:

aa) LA EXPRESIÓN "*WITHOUT RIGHT*"

Por una parte, el tipo objetivo requiere que la conducta se lleve a cabo ilícitamente o *without right*. Esta idea mantiene la línea ya apuntada por la Recomendación (89) 9, que sustituyó la expresión sin autorización (*unauthorized access*) por la de ilícitamente (*without right*). Según sus redactores, esta expresión permite englobar tanto los casos en que la prohibición al acceso se deriva directamente de una disposición legal imperativa cuanto aquellos en los que éste depende de la voluntad dispositiva del usuario legítimo del sistema[111]. Lo anterior supone la atipicidad de aquellos accesos en los que existe el consentimiento del propietario u otro accedente legítimo del sistema o de parte del mismo, así como de aquellos casos en los que el sistema sea de acceso libre o abierto al público[112].

---

[111] En este concreto apartado el Informe Explicativo puntualiza que el término ilegítimo debe ser interpretando en el plano del contexto en que se plantea la posible ilicitud del acceso, de tal forma que –sin pretensión de restringir la aplicación de este concepto por parte de los Estados conforme a su Derecho interno– entiende que deben resultar incardinables en él todas aquellas situaciones en las que el acceso se lleva a cabo sin tener facultades para ello (ya sean de orden legislativo, ejecutivo, administrativo, judicial, contractual o consensual) o en ningún modo amparado por justificaciones, excusas y defensas legales establecidas o por principios pertinentes con arreglo a las leyes nacionales. A tal efecto, indica que el Convenio no afecta a las conductas legítimas de un Gobierno cuando éste interviene para mantener el orden público, proteger la seguridad nacional o investigar los delitos, ni a las actividades legítimas y comunes inherentes al diseño de las redes o a prácticas comerciales que no deben ser consideradas delitos como es, en este caso concreto, los enlaces de hipertexto, incluidos los *cookies*, que permiten el acceso a una página web. COUNCIL OF EUROPE, 2001: 12-14 párrafos 38-48.

[112] COUNCIL OF EUROPE, 2001: 14 párrafo 47.

bb) VULNERACIÓN DE MEDIDAS DE SEGURIDAD

Por otra parte, se preve la posibilidad de incluir como elemento del tipo objetivo la vulneración de medidas de seguridad. No obstante, cabe recordar que se trata de un elemento cuya introducción es facultativa para los Estados. Lo anterior supone una variación sustancial de la conducta en relación con la Recomendación, que integraba (obligatoriamente) este elemento en el tipo objetivo, y se aproxima más al Informe *Computer-related Crime* de la Organización para la Cooperación y Desarrollo Económico, que le atribuía un carácter facultativo.

En realidad, el Convenio propone la incriminación de una disposición normativa con un contenido de injusto menor que la Recomendación o el Informe, teniendo en cuenta que su introducción en la tipicidad objetiva supondrá una considerable restricción de los supuestos subsumibles en el tipo. Lo anterior convierte a este elemento en uno de los factores fundamentales de la propia descripción típica. Aún así, el Comité redactor deja patente que los países que ya disponían de regulación en materia de delincuencia informática han introducido ya esta exigencia en la redacción típica al seguir las directrices de la Recomendación y algunos algunos de los que no lo han hecho la incluirán al considerar que la mera intrusión en un sistema no crea un peligro suficientemente relevante para necesitar la intervención del Derecho penal[113].

b) PARTE SUBJETIVA DEL TIPO

El Convenio restringe la parte subjetiva del tipo a la modalidad puramente dolosa[114]. En cambio, es posible añadir elementos subjetivos específicos al dolo del autor: la finalidad de obtener datos informáticos u otra finalidad deshonesta[115].

---

[113] COUNCIL OF EUROPE, 2001: 15 párrafo 49.

[114] COUNCIL OF EUROPE, 2001: 12 párrafo 39.

[115] Se recupera en este punto la redacción utilizada en el Informe de la OCDE, que había sido abandonada por la Recomendación (89) 9 pero sí considerada como una opción. Véase apartados II y III de este Capítulo.

VIII. NORMATIVA APROBADA POR LA UNIÓN EUROPEA

La Unión Europea también se hizo eco de la necesidad de armonizar la normativa nacional en materia de delincuencia informática pero, teniendo en cuenta las limitaciones a las que la organización se encontraba sometida en el momento en relación con la adopción de normativa vinculante en Derecho penal, sus primeros pasos tuvieron lugar tímidamente a través de comunicaciones.

A) PRELIMINARES: LAS COMUNICACIÓNES

La primera Comunicación que en tal sentido se aprobó es la *eEurope - An information society for all* de 8 de diciembre de 1999, a través de la que crea *eEurope*, un espacio de integración digital de carácter global.

Posteriormente, el 26 de enero 2001 la Comisión publicó otra comunicación: *Creating a Safer Information Society by Improving the Security of Information Infrastructures and Combating Computer-related Crime* con la finalidad de adoptar medidas eficaces en el ámbito penal para enfrentarse a las amenazas *in crescendo* derivadas del fenómeno informático[116]. Con este mismo cometido, propuso en ella la redacción de una Decisión Marco que contribuyera a fomentar la armonización del Derecho penal sustantivo en la materia[117].

Apuntando en esta misma dirección, la Comisión publica también la Comunicación de 6 de junio de 2001 sobre *Network and Information Security - A European Policy approach*[118].

---

[116] En este sentido, considera que los delitos informáticos constituyen una amenaza para las inversiones y activos industriales, así como para la seguridad y la confianza de la sociedad de la información, de forma que únicamente el establecimiento de los medios necesarios para una cooperación eficaz entre los distintos Estados sería el elemento fundamental para el establecimiento de un contexto de libertad, seguridad y justicia. EUROPEAN UNION COMISSION, 2001: 23.

[117] EUROPEAN UNION COMISSION, 2001: 31-32.

[118] EUROPEAN UNION COMMISSION, 2001: 31-32.

B) DECISIÓN MARCO 2005/222/JAI, DEL CONSEJO, DE 24 DE FEBRERO, RELATIVA A LOS ATAQUES A SISTEMAS DE INFORMACIÓN

La proposición de la Comunicación de 2001 tuvo sus frutos en la creación de una Comisión para la redacción de dicha Decisión Marco. Tras la redacción de varios borradores, se aprobó finalmente la Decisión Marco 2005/222/JAI, del Consejo de la Unión Europea, de fecha 24 de febrero de 2005, relativa a los ataques a los sistemas de información.

1. ESTRUCTURA

La estructura y la redacción de la Decisión es muy similar a la del Convenio, si bien con un contenido más reducido, pues consta tan solo de un Preámbulo y un conjunto de 13 artículos, el primero de ellos dedicado a las Definiciones, y de los restantes, solo en tres se describen conductas que los Estados deben tipificar, mientras que en los demás se prevén cuestiones de carácter accesorio y procesal.

Los delitos cuya transposición se reclama son los de acceso ilegal a los sistemas de información, intromisión ilegal en los sistemas de información e intromisión ilegal en los datos que, respectivamente, se corresponden con las conductas de acceso ilícito (artículo 2), ataques a la integridad del sistema (artículo 5) y ataques a la integridad de los datos (artículo 4).

2. ACCESO ILÍCITO

El artículo 2, relativo al *Acceso ilegal a los sistemas de información*, reza lo siguiente: *Cada Estado miembro adoptará las medidas necesarias para que el acceso intencionado sin derecho a la totalidad o a una parte del sistema de información sea sancionable como delito, al menos en los casos de menor gravedad*[119].

---

[119] *"Article 2. illegal access to information Systems 1. Each Member State shall take the necessary measures to ensure that the intentional access without right to the whole or any part of an information system is punishable as a criminal offense, at least for cases which are not minor".*

Igual que ya hacía el Convenio, la Decisión recoge la facultad de que cada Estado miembro decida si la conducta debe ser punible *únicamente delito cuando se realice infringiendo medidas de seguridad*[120].

a) TIPO OBJETIVO

El contenido de la propuesta de tipificación en relación con el acceso ilícito es la misma que la ofrecida por el Convenio, pues la definición coincide en sus elementos con la proporcionada por éste, que, a su vez, proviene de la Recomendación. La única diferencia entre ambas normas reside en que la opción que el Convenio concede a los Estados miembros de añadir ulteriores exigencias para configurar la conducta se reduce a una sola posibilidad: la infracción de medidas de seguridad.

b) OBJETO MATERIAL

Por lo que al objeto material respecta, aunque en general la Decisión Marco también se refiere a los sistemas de información y a los datos informáticos como objetos de los delitos cuya incriminación propone, en el acceso ilícito éste continúa siendo el sistema informático. No obstante, la Decisión no utiliza la expresión sistema informático sino la de sistema de información. Teniendo en cuenta lo anterior, se presenta como necesario dilucidar si el concepto de sistema de información contenido en la Decisión Marco resulta equiparable a la noción de sistema informático que venía recogida en la normativa aprobada hasta el momento o si por el contrario de la Decisión se desprende una divergente significación de uno y otro término. Para ofrecer una respuesta a la cuestión planteada habrá que acudir al conjunto normalizado de definiciones que la Decisión recoge en su Artículo 1 sobre los conceptos que utilizará a lo largo del todo el articulado.

---

[120] *"... 2. Each Member State may decide that the conduct referred to in paragraph 1 is incriminated only where the offense is committed by infringing a security measure".*

La Decisión Marco ofrece una definición de sistema de información, de datos informáticos, de persona jurídica y de la expresión ilícitamente (*without right*). Si se atiende a los conceptos que describe, de entrada, se observa que los términos en relación con los cuales se recoge una noción jurídica no se corresponden exactamente con los que aparecen en el Convenio. Así, por ejemplo, éste no aclara el término *persona jurídica*. Ambas especifican, en cambio, qué debe entenderse por sistema de información y por datos informáticos, motivo por el cual es posible un análisis comparativo de ambos conceptos.

i) NOCIÓN DE SISTEMA DE INFORMACIÓN

La Decisión Marco ofrece, pues, una noción de sistema de información, definiéndolo como *todo dispositivo o grupo de dispositivos interconectados o relacionados entre sí, uno o varios de los cuales realizan, mediante un programa, el tratamiento automático de datos informáticos, así como los datos informáticos almacenados, tratados, recuperados o transmitidos por estos últimos para su funcionamiento, utilización, protección y mantenimiento.*

En términos generales, puede decirse que esta conceptualización de sistema de información es la misma que la recogida en el Convenio para la noción de sistema informático, por lo que *a priori* ambos términos deben considerarse sinónimos. Comparando una y otra norma puede decirse, asimismo, que la Decisión acoge una descripción más completa de dicho término, ya que menciona expresamente cuáles son las funciones específicas de los programas informáticos: el almacenamiento, tratamiento, recuperación y transmisión de los datos, y les atribuye una serie de características básicas: conseguir el funcionamiento del sistema a través de la utilización, la protección y el mantenimiento de los datos informáticos. Según la Decisión Marco el programa informático conforma claramente, en consecuencia, el eje motor del sistema de información.

ii) NOCIÓN DE DATOS INFORMÁTICOS

En cuanto al concepto de datos informáticos, lo describe del siguiente modo: *Toda representación de hechos, informaciones o conceptos expresados 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*.

A diferencia de lo que sucede con la definición de sistema informático-información, la noción de datos informáticos es idéntica a la que recoge el Convenio. Por consiguiente, la Decisión Marco engloba igualmente dentro del concepto legal de datos informáticos tanto a los datos *stricto sensu* como a los programas informáticos.

c) LA EXPRESIÓN *WITHOUT RIGHT*

Como se ha indicado, la Decisión Marco prevé idénticos elementos que el Convenio por lo que se refiere a la tipicidad, reduciendo las posibilidades de opción de los países al añadir únicamente como elementos adicionales a uno: la vulneración de medidas de seguridad. Respecto de éstas últimas, nada comenta al respecto pero sí define la primera. Queda, por tanto, comentar la expresión *without right*.

La Decisión Marco entiende por tal *el acceso o interferencia no autorizada por el propietario, por el titular de otro derecho sobre el sistema o parte de él, o no permitida por la legislación nacional*. Según se ha expresado con carácter precedente[121], no resultan de todo punto equiparables los términos *sin derecho* y *sin autorización* en tanto traducciones posibles de la ya mencionada expresión inglesa *without right*. Esta idea viene a ser confirmada, además, por la definición enunciada en la Decisión Marco, que da la razón a este trabajo cuando afirma que la expresión *without right* posee un contenido más amplio que el que pueda tener la ausencia de autorización.

---

[121] Véase Apartado III de este Capítulo.

C) 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

La pugna existente entre la Comisión y el Consejo de la Unión Europea sobre la aprobación de regulación comunitaria en materia penal condujo a que la Decisión Marco 2005/222/JAI, del Consejo de la Unión Europea, de fecha 24 de febrero de 2005, relativa a los ataques a los sistemas de información, fuera sustituida por 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.

La Directiva mantiene el mismo objetivo que la Decisión Marco y que las restantes normas que la precedieron en cuanto a la aproximación de las normas de Derecho penal de los Estados miembros en materia de ataques contra los sistemas de información, mediante el establecimiento de unas normas mínimas destinadas a la definición de las infracciones penales y las sanciones aplicables, y mejorar la cooperación entre las autoridades competentes[122]. No obstante, la Directiva no se conforma con incorporar el articulado de la Decisión Marco a los efectos meramente de transfigurar su naturaleza normativa, sino que establece como objetivo modificar y ampliar las disposiciones contenidas en ésta a fin de ofrecer un nuevo y actualizado enfoque frente a la delincuencia informática y la ciberdelincuencia[123]. Es por ello que, de hecho, sustituye a ésta en la totalidad de sus términos[124].

---

[122] Considerando (1) de la Exposición de Motivos y Artículo 1.

[123] Considerando (34) de la Exposición de Motivos.

[124] En el Considerando (34) in fine explica que: *Dado que las modificaciones necesarias son importantes, tanto por número como por su naturaleza, la Decisión marco 2005/222/JAI debe, en aras de la claridad, ser sustituida en su totalidad en relación con los Estados miembros que participan en la adopción de la presente Directiva.*

1. ESTRUCTURA

La Directiva mantiene en general la estructura de la Decisión Marco, previendo un contenido más reducido que el Convenio aunque más amplio que la Decisión Marco. Consta de un total de 19 artículos, el primero de ellos dirigido a fijar el Objeto de la Directiva, el segundo dedicado a las Definiciones, nueve más conteniendo el Derecho penal material y los restantes sobre cuestiones de carácter accesorio y procesal.

Los delitos cuya transposición se reclama son los de acceso ilegal a los sistemas de información, intromisión ilegal en los sistemas de información e intromisión ilegal en los datos que, respectivamente, se corresponden con las conductas de acceso ilícito (artículo 3), interferencia ilegal en los sistemas de información (artículo 4), interferencia ilegal en los datos (artículo 5), interceptación ilegal (artículo 6) y los instrumentos utilizados para cometer las infracciones (artículo 7).

2. ACCESO ILÍCITO

En esta ocasión es el artículo 3 el que propone la punición del acceso ilícito: *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*.

a) TIPO OBJETIVO

i) CONDUCTA TÍPICA

La conducta típica se mantiene inalterada por lo que respecta a la normativa precedente, aunque incorpora un cambio de extrema relevancia: el criterio objetivo relativo a la vulneración de las medidas de seguridad deja de ser un elemento de introducción facultativa para los Estados para pasar a formar parte del tipo objetivo mínimo cuya incriminación se reclama.

ii) OBJETO MATERIAL

El objeto material continúa siendo el sistema de información y no el sistema informático. La Directiva entiende a este efecto que los sistemas de información son un elemento esencial para la interacción política, social y económica en la Unión[125] y establece en su artículo 3 un conjunto de definiciones comunes a fin de garantizar la aplicación coherente de la misma en los Estados miembros[126]: las de sistema de información, datos informáticos, persona jurídica y la expresión sin autorización.

Como puede observarse las definiciones son exactamente las mismas que las contenidas en la Decisión Marco. Así pues, el apartado a) describe *sistema de información* como *todo aparato o grupo de aparatos interconectados o relacionados entre sí, uno o varios de los cuales realizan, mediante un programa, el tratamiento automático de datos informáticos, así como los datos informáticos almacenados, tratados, recuperados o transmitidos por dicho aparato o grupo de aparatos para su funcionamiento, utilización, protección y mantenimiento*; y la letra b) «datos informáticos» como *toda representación de hechos, informaciones o conceptos de una forma que permite su trata miento por un sistema de información, incluidos los pro gramas que sirven para hacer que dicho sistema de información realice una función.*

iii) LA EXPRESIÓN SIN AUTORIZACIÓN

La letra d) del artículo 3 define qué debe entenderse por cometer la infracción *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*.

---

[125] Considerando (2)

[126] Considerando (7)

D) OTRAS ACTUACIONES DE LA UNIÓN EUROPEA

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, constituyó la apuesta definitiva por parte de la Unión Europea para la lucha contra la delincuencia informática. Desde entonces, la Unión Europea ha seguido trabajando en la materia con la finalidad de lograr una adecuada articulación de los mecanismos para combatir este tipo de delincuencia.

Así, el 22 de mayo de 2007 la Comisión presentó la Comunicación *Hacia una estrategia general en la lucha contra el ciberdelito*, en la que determinaba como prioridades en este campo la lucha contra el material de abuso sexual sobre menores en Internet y acciones para hacer frente a ataques masivos contra los sistemas de información y contra el fraude de identidad.

Con este mismo fin publicó la Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones, de 30 de marzo de 2009, sobre protección de infraestructuras críticas de información: Proteger Europa de ciberataques e interrupciones a gran escala: aumentar la preparación, seguridad y resistencia.

IX. VALORACIÓN PERSONAL

De la aprobación de la normativa vinculante en materia de delincuencia informática se desprenden dos consecuencias para la tipificación del acceso ilícito en los Estados parte/miembros:

En primer lugar, el delito de acceso ilícito es delito en todos los Estados miembro de la Unión Europea y parte en el Consejo de Europa además de en todos aquellos países que, no siendo parte en ninguna de las organizaciones anteriores, hayan ratificado el Convenio sobre Cibercriminalidad de 2001. Aquellos países que ya disponen de regulación en la materia deberán modificar ésta para adaptarla a las normas vinculantes a las que se ha hecho referencia, mientras que los que no hubieran aprobado ya disposiciones al respecto, deberán regular la materia *ex novo*, como en el caso de España.

En segundo lugar, la previsión de elementos de introducción facultativa posibilita que el alcance de la incriminación varíe para cada Estado que sea parte en el Convenio sobre Cibercriminalidad, pero este margen será menor en el caso de los Estados miembro de la Unión. El Convenio (también la Decisión Marco) establece una regulación de mínimos solicitando que se castigue el mero acceso a un sistema informático, siendo elementos facultativos la vulneración de las medidas de seguridad, la exigencia de un ánimo subjetivo en el autor o la interconexión de los sistemas. En cambio, la Directiva obliga a los Estados a incriminar el acceso ilícito vulnerando medidas de seguridad como conducta básica, sin conceder a los Estados ningún margen de elementos de introducción facultativa. El punto de partida del Convenio es más amplio, pero las restricciones a las que permite llegar son mayores que las que propone la Directiva, hecho que puede crear importantes divergencias entre las legislaciones de los países. Desde esta perspectiva, aunque el Convenio concede un nivel mayor de libertad a los Estados parte en el mismo a la hora de tipificar el acceso ilícito, la Directiva parece culminar mejor las expectativas de uniformidad nacional.

X. APLICACIÓN DEL CONVENIO Y LA DIRECTIVA

Tomando en consideración conjuntamente las dos normas de carácter vinculante citadas, se desprende que, por un lado, todos los Estados miembros de la Unión Europea deberán tipificar el delito de acceso ilícito añadiendo como requisito la vulneración de las medidas de seguridad, mientras que los países que hayan ratificado el Convenio sobre Cibercrimen podrán optar entre incluirlo no. Ello puede conducir a una legislación totalmente divergentes. A continuación se presunta un estudio pormenorizado de todos los países en los que dichas normas son de aplicación:

A) TABLA DE APLICACIÓN DEL DELITO DE ACCESO ILÍCITO

	A	M/EA	MS	OM	ESI	ART/§
ALBANIA	X	EA	X	SI		192/b
ALEMANIA	X	-	X	D		§202 a)
ANDORRA	X	-	X	SI		182.2
ARMENIA	X	-	X	D+SI		251
ARGENTINA						
AUSTRALIA	X	-	X	D		§478.1
AUSTRIA	X	-	X	D/SI	B	§118a
AZERBAIJAN	X	-	X	I		271
BÉLGICA	X	M	-	SI	-	550*bis* § 1er
BOSNIA Y H.	X	-	X	SI/R	-	397
BULGARIA	X	-	-	D	-	319a
CANADA	X	X	-	CS	-	342.1 (1)
CHILE						

	A	M/EA	MS	OM	ESI	ART/§
CHIPRE	X		-	SI	-	4 L. 22(III) 4
COLOMBIA						
COSTA RICA						
CROACIA	X	-	-	SI/D	-	266
DINAMARCA	X	-	-	I	-	§ 263 (2)
ESLOVAQUIA	X	-	-	I	B/P	§ 247
ESLOVENIA	X	-	-	SINF	-	221
ESPAÑA	X	M	X	SI	-	197.1 *bis*
ESTONIA	X	-	X	SI	-	§ 217 (1)
ESTADOS UNIDOS	X	EA	X	C	-	§ 1030
FILIPINAS	X	-	-	SI	-	§ 33 ECA
FINLANDIA	X	-	X	SI	-	§ 8 C. 38
FRANCIA	X	M	-	STAD	-	323-1
GEORGIA	X	-	-	I	-	284
GRECIA	X	-	-	D	-	370C§2
HOLANDA	X	-	-	STAD	-	138a
HUNGRÍA	X	-	X	SINF	-	§ 423
IRLANDA	X	-	-	C	B/P	§ 9 TFA
ISLANDIA	X	-	-	D	-	228
ISRAEL						
ITALIA	X	M	X	SI	-	615 *ter*

	A	M/EA	MS	OM	ESI	ART/§
JAPÓN	X	-	X	C		3 L. 128 1999
LETONIA	X	-	X	STAD		§ 241
LIECHTENSTEIN	Ratificación 27.01.2016 - Entrada en vigor 01.05.2016					
LITUANIA	X	-	X	SINF	-	198(1)
LUXEMBURGO	X	M	-	STAD	-	509-1
MALTA	X	-	-	D	-	337C (1) (a)
MAURICIO (ISLAS)	X	-	-	C	CS	5 CMCA2003
MARRUECOS						
MÉXICO						
MOLDAVIA	X	EA	-	D	C/D	259
MONACO	Firma					
MONTENEGRO	X	-	X	C	-	355
NORUEGA	X	-	X	D		145
PANAMA	-	-	-	-	-	-
POLONIA	X	-	X	SINF	-	267 § 1
PORTUGAL	X	-	-	SI	-	6 L. 109/2009
RUMANIA	X	-	-	SI	-	42 L. 161/2003
RUSIA						
SAN MARINO						
SENEGAL						
SERBIA	X	-	X	C/D	-	112

	A	M/EA	MS	OM	ESI	ART/§
SRI LANKA	X	-	-	C	-	3 L n. 24 2007
SUDÁFRICA	FIRMA 23.11.2001					
SUECIA	FIRMA 23.11.2001					
SUIZA	X	-	X	STAD	-	143 *bis*
REINO UNIDO	X	-	-	C	P/D	1 (1) CMA
R. CHECA	X	-	-	SI	-	§ 257 (a)
R. MACEDONIA	X	-	-	C	P/D	251 (1)
R. DOMINICANA	X	-	-	SINF	-	6 Ley n. 53-07
TURQUÍA	X	M	-	STAD	-	243-(1)
UKRANIA	-	-	-	-	-	-

> LEYENDA

- Estados miembros tanto del Consejo de Europa como de la Unión Europea

- Países no miembros del Consejo de Europa pero parte en el Convenio

- Estados miembros únicamente del Consejo de Europa

> ABREVIATURAS

A	Acceso	**ESI**	E. subjetivo injusto	**SINF**	Sistema Información
B	Beneficio	**M**	Mantenimiento	**SATD**	Sistema Automatizado Tratamiento Datos
C	Ordenador	**MS**	Medidas Seguridad		
CS	Computer Service	**OM**	Objeto Material	**ART / §**	Artículo / Sección
D	Datos	**P**	Perjuicio	**X / -**	Con / Sin regulación
EA	Exceso autorización	**SI**	Sistema Informático	/ +	o / y

B) DEFINICIÓN DE SISTEMA Y DATOS INFORMÁTICOS

Pasando a analizar las concretas nociones de sistema informático y datos informáticos… Como se ha visto, los Estados no están obligados a adoptar definiciones idénticas a las previstas por el Convenio, ostentando, por tanto, cierta discrecionalidad a la hora de implementar tales conceptos siempre y cuando éstos se encuentren dentro de los márgenes fijados por el artículo 1 del Convenio de Cibercrimen.

El Informe del Consejo de Europa relativo a la aplicación del Convenio sobre Cibercrimen aconseja que los Estados que no dispongan todavía de normativa en la materia, realicen los actos legislativos necesarios para cubrir esta laguna que, según los expertos, podría representar un serio obstáculo por la uniforme interpretación y aplicación de los comunes infracciones penales a nivel internacional[127].

Aun así, no todos los países han positivizado una definición de los términos contenidos en el Convenio, aunque, los que lo han hecho, han seguido la definición contenida en éste. Lo lógico sería que los países que adoptan como objeto material del delito hubieran conceptuado el sistema informático, mientras que aquellos que hubieran acogido los datos informáticos como tal se hubieran centrado principalmente en estos.

El punto fuerte de discrepancia entre los distintos Estados lo ha constituido el objeto material del delito. A continuación, se presenta con detalle como se ha manifestado esta distinta regulación de los Estados.

[127] PICOTTI y SALVADORI, 2008: 12.

No definen sistema Albania[128], Armenia[129], Australia[130],

[128] **ALBANIA.** Aunque el artículo 192/b del Código penal albano no recoge una definición de sistema informático, distingue entre un tipo básico con pena de prisión de hasta tres años en el que se castiga el acceso a todo o parte de un sistema informático cualquiera y un subtipo agravado con prisión de hasta 10 años para un conjunto de sistemas informáticos considerados para el legislador de interés público, citando expresamente aunque solo a modo ejemplificativo los relativos a militar, de seguridad nacional, de orden público, de protección civil o de sanidad.

[129] **ARMENIA.** El artículo 251 Código penal de Armenia, que tampoco ofrece una definición de sistema informático, tiene como objeto material del delito el propio sistema de información como la propia información almacenada en el sistema, una red o un medio de almacenamiento.

[130] **AUSTRALIA.** Aun a pesar de que Australia ha dedicado una Sección específica de su Código penal, la 476.1, a ofrecer un conjunto de definiciones en materia de delincuencia informática, como cabe recordar, incrimina la conducta de acceso ilícito siguiendo la tendencia de Alemania o España -ésta última entre 2010 y 2015- adoptando como objeto material no el sistema sino los datos informáticos. En coherencia con ello, no recoge expresamente una definición de sistema informático pero es que, de hecho, ni la Sección 476.1, ni la 477.1, que describen la infracción penal, hacen referencia a dicho concepto, aludiendo en todo caso al de ordenador o *computer*. No obstante, tras la derogación a través de la *Cybercrime Legislation Amendment Act* de 2012 de la única definición próxima a las exigidas por el Convenio, la de ordenador de la Commonwealth como una computadora en propiedad, arrendada u operada por una entidad de la Commonwealth, puede encontrarse una definición de lo que debe entenderse por *computer* en la redacción vigente de la Sección 22 de la Australian Security Intelligence Organisation Act de 1979, que afirma que debe entenderse como tal una o más ordenadores, uno o más sistemas informáticos, una o más redes informáticos o cualquier combinación de los anteriores. En consecuencia, si este país decidiera afrontar la reforma del Código penal para adaptarlo a las exigencias de la Convención, la noción de ordenador ya recogida en su legislación vigente ya se adaptaría plenamente a la requerida por la Convención.

Azerbaiján[131], Bélgica[132], Croacia[133], Dinamarca[134], Eslovaquia[135],

[131] **AZERBAIJÁN.** De hecho, el Código penal de Azerbaiján no castiga el acceso ilícito. Tan solo se castiga en el artículo 271 el acceso ilícito a información electrónica-informática y, aunque el apartado 2.2 hace referencia a tener acceso al ordenador, el sistema informático o su red, tanto la parte *ab inicio* del apartado alude a la posibilidad de entender al funcionario público sujeto activo como la cláusula general introductoria del apartado -la cual se refiere a cometer el acceso a la información con las condiciones expresadas en el apartado 2- hacen descartar esta posibilidad.

[132] **BÉLGICA.** El artículo 550 bis del Código penal Belga recoge como objeto material del delito el sistema informático, aunque sin ofrecer ninguna definición del mismo.

[133] **CROACIA.** Croacia, que forma parte de los Estados que ofrece protección tanto al sistema como a los datos en el artículo 266 (1) protege tanto los datos informáticos como el propio sistema informático, dispensando el párrafo (2) tutela especial a través de un subtipo agravado a los sistemas informáticos del Gobierno, Instituciones Públicas o de una empresa de especial interés público. A tal efecto, el artículo 87 ítem 17 define sistema informático como cualquier dispositivo o grupo de dispositivos interconectados o relacionados entre sí, uno o más de los cuales, en virtud de un programa. No obstante, dentro de la propia definición de sistema informático incluye los datos que en él se almacenan, manipulan, cargan o transfieren a los efectos del trabajo y su uso, protección y mantenimiento.

[134] **DINAMARCA.** Cabe recordar que la Sección 263 párrafo 2 no tiene como objeto material el sistema informático sino que castiga el acceso a la información y a los programas contenidos en el mismo, ello sin hacer referencia al concepto de sistema informático sino al de sistema de información.

[135] **ESLOVAQUIA.** Aunque el Código penal eslovaco no define qué debe entenderse por sistema informático, la Sección 247 (1) del mismo recoge el sistema informático como objeto material del delito.

Eslovenia[136], Estonia[137], Finlandia[138], Francia[139], Georgia[140], Grecia[141], Hungría[142], Islandia[143], Italia[144], Japón[145], Letonia[146], Lithuania[147],

---

[136] **ESLOVENIA.** El artículo 221 del Código penal de Eslavonia recoge el acceso al sistema informático sin establecer ningún tipo de definición del mismo.

[137] **ESTONIA.** La Sección 217 (1) del Código penal estonio establece un tipo básico en el que el objeto material es el sistema informático. Sin embargo, el párrafo (2) establece unan protección agravada para los sistemas que contienen secretos de Estado, información clasificada o información prescrita para uso oficial, así como aquellos vinculados a un sector vital.

[138] **FINLANDIA.** La Sección 8 del Capítulo 38 del Código penal finlandés protege, aunque sin ofrecer ninguna definición, ofrece protección tanto al sistema informático como a la información contenida en él.

[139] **FRANCIA.** En Francia el artículo 323-1 del Código penal hace referencia a ***système de traitement automatisé de données***, es decir, sistema de tratamiento automatizado de datos personales y no a sistema informático.

[140] **GEORGIA.** En artículo 284 del Código de Georgia no castiga el acceso a datos sino el acceso al sistema sino el acceso a la información contenida en el sistema.

[141] **GRECIA.** Cabe recordar que el Código penal griego ni siquiera recoge como objeto material el sistema informático en su artículo 370B y Γ.

[142] **HUNGRÍA.** La Sección 423 párrafo 1 del Código penal húngaro hace referencia como objeto material al **sistema de información** y no al sistema informático. la Sección 300/C (1) recoge el sistema informático y la red informático como objeto material del delito.

[143] **ISLANDIA.** La Sección 1 del artículo 228 no tutela el acceso al sistema informático, sino a los datos y programas informáticos.

[144] **ITALIA.** A pesar de que el Código penal italiano no solo fue uno de los pioneros en proteger la integridad del sistema informático, no recoge a día de hoy una definición de sistema informático.

[145] **JAPÓN.** Aunque la Ley número 128 de 1999 hace referencia al término ordenador, pero sin recoger en su articulado ninguna definición del mismo.

[146] **LETONIA.** La Sección 241 (1) hace referencia a ***automated data processing system***, es decir, a un sistema de procesamiento automático de datos.

[147] **LITUANIA.** El artículo 198 del Código penal lituano hace referencia a sistema de información, no ofreciendo definición del mismo, pero previendo una forma agravada en su apartado 2 para tutelar los sistemas de estratégica importancia para la seguridad nacional, o pertenecientes al Gobierno del Estado, la economía o el sistema financiero.

Luxemburgo[148], Moldavia[149], Noruega[150], Polonia[151], la República Checa[152], Reino Unido[153], Suiza[154], Turquía[155] y Ucrania[156].

---

[148] **LUXEMBURGO.** El artículo 509-1 del Código penal de Luxemburgo recoge una expresión similar a la prevista en el Código penal francés: ***système de traitement ou de transmission automatisé de données***, es decir, sistema de tratamiento o de transmisión automatizada de datos.

[149] **MOLDAVIA.** El artículo 259 del Código penal moldavo adopta como objeto material del delito el concepto de información, entendiendo englobados dentro de éste los datos informáticos, los dispositivos de almacenamiento de datos, los sistemas informáticos y las redes informáticas.

[150] **NORUEGA.** La Sección 145 y 145 b del Código penal noruego no castiga, de hecho, el acceso al sistema, sino el acceso a los datos o al software.

[151] **POLONIA.** Tras la reciente modificación operada en 2015, el artículo 267 sección 2 del Código penal polaco recoge como objeto material el **sistema de información**, si bien no define qué debe entenderse como tal.

[152] **REPÚBLICA CHECA.** Aunque no recoge una definición de sistema informático, la Sección 230 (1) del Código penal checo adopta como objeto material único del delito de acceso el sistema informático.

[153] **REINO UNIDO.** La *Computer Misuse Act* de 1990 castiga en su artículo 2 el acceso no autorizado a **material informático**, de modo que no incrimina expresamente el acceso ilícito a un ordenador sino el acceso ilícito a material informático. No obstante, de su redacción se desprende que, en realidad, sí que está criminalizando el contenido del acceso, puesto que acceder ilícitamente a un ordenador supone conseguir que éste realice alguna función por medio de algún programa o dato que permita al intruso tener acceso él. Además, exige que éste acceso se realice sin autorización y con conocimiento de que se está accediendo, aunque sin ninguna intención subjetiva añadida más

[154] **SUIZA.** El artículo 143 castiga desde 2010 el acceso ilícito a un **sistema de procesamiento de datos**, sin establecer definición alguna de lo que debe entenderse como tal.

[155] **TURQUÍA.** Aun a pesar de que el artículo 243 párrafo 1 protege el **sistema de procesamiento de datos** y el artículo 2 de la Ley nº 5651 de 4 de mayo 2007 adoptó una serie de definiciones en materia de criminalidad informática, la de sistema no se encuentra entre ellas.

[156] **UCRANIA.** El Código penal ucraniano no sólo no establece una definición, sino que además ni siquiera castiga el acceso ilícito, sino la interferencia en el sistema o la red informática, conducta prevista en el artículo 361.1 en la que es el sistema el objeto material del delito.

Sí han introducido una definición Austria[157], Bosnia y Herzegovina[158], Bulgaria[159], Canadá[160], Chipre[161], o Estados

[157] **AUSTRIA.** La Sección 118 a del Código penal austríaco recoge como objeto material del delito el sistema informático, mientras que la Sección 74 párrafo 8 del Código penal austríaco define sistema informático, en el marco de lo dispuesto por el Convenio, como el dispositivo o conjunto de dispositivos combinados entre sí que tienen como función el procesamiento asistido de procesamiento de datos.

[158] **BOSNIA Y HERZEGOVINA.** En el caso de Bosnia y Herzegovina la transposición del Convenio sobre Cibercrimen se ha llevado a cabo de una forma muy dispersa a través de distintas normas. Es pues, en el Código de Procedimiento penal donde se encuentra tanto una definición de sistema informático como una conceptualización de datos informáticos. Por lo que aquí interesa, define sistema informático como cualquier dispositivo o un grupo de dispositivos mutuamente conectados o vinculados, de los cuales uno o más de uno están procesando automáticamente los datos sobre la base de un programa. Sin embargo, ninguno de los Códigos en materia penal hace referencia específica a dicho concepto. Así, el artículo 397 del Código penal federal del país hace referencia a un sistema o a una red electrónicos de procesamiento de datos; el artículo 292d) del Código penal de la Republika Srpska a un ordenador, red de ordenadores o procesos electrónicos de datos; y el del Brčko District a un sistema i red para el procesamiento electrónico de datos.

[159] **BULGARIA**. Como se ha puesto de manifiesto en el apartado anterior, Bulgaria centra la atención en los datos y no en el sistema, aunque ofrece una definición de sistema computerizado en el artículo 93 ítem 21 del Código penal: cualquier dispositivo o grupo de dispositivos interconectados o vinculados, uno o más de los cuales, por medio de un programan, realizan el procesamiento automático de datos.

[160] **CANADA.** Canadá, uno de los países pioneros en la incriminación de la delincuencia informática no ha ratificado la Convención hasta el año 2015. En este sentido, el artículo 342.1, reformado recientemente, no castiga directamente el acceso al sistema informático, pero sí que ofrece un conjunto amplio de definiciones entre las que se encuentra el concepto de sistema informático: Sistema informático significa un dispositivo que, o un grupo de dispositivos interconectados o relacionados uno o más de los cuales,

(A) contiene los programas de ordenador u otros datos, y
(B) de conformidad con los programas de ordenador,
(i) realiza la lógica y de control, y
(ii) puede llevar a cabo cualquier otra función;

[161] **CHIPRE.** Chipre introdujo mediante el instrumento de ratificación de la Convención, la Ley nº 22 (III) 04, idénticas previsiones a las dispuestas en el articulado de ésta, tanto por lo que se refiere a las definiciones como en lo que concierne a las conductas punibles. Así pues, la legislación del país dispone de una transposición directa con nimias variaciones de todas y cada una de las definiciones (artículo 2) y conductas (artículo 4) propuestas, siendo, por tanto, el sistema informático el objeto material del delito.

Unidos[162], Holanda[163], Malta[164], Montenegro[165], Portugal

[162] **ESTADOS UNIDOS DE AMERICA.** La Sección 1030 (e) (1) del Código penal federal de Estados Unidos hace referencia al concepto de ordenador, que podría equipararse al de sistema informático: un sistema electrónico, magnético, óptico, electroquímico, u otro dispositivo de procesamiento de datos de alta velocidad de la realización, funciones aritméticas o lógicas de almacenamiento, e incluye cualquier tipo de instalación de almacenamiento de datos o comunicaciones directamente relacionadas o que opera en conjunción con dicho dispositivo , pero este término no incluye una máquina de escribir automatizado o máquina de componer, una calculadora de mano transportable, u otro dispositivo similar.

[163] **HOLANDA.** La Sección 138ab del Código penal holandés hace referencia a dispositivos informáticos y sistemas informáticos (previendo un tipo agravado para aquellos casos en los que se trata de un acceso por medio de una red de telecomunicación pública), cuya conceptualización se la Sección 80 sexies define como una instalación para el almacenamiento, procesamiento y transmisión de datos por medios electrónicos.

[164] **MALTA.** El Código penal maltés ofrece en el artículo 337B (1) una amplia lista de definiciones, entre las que se incluyen las de ordenador, sistema informático y sistema de información. Sin embargo, el objeto material del delito serán únicamente los datos, el software y la documentación de soporte, castigándose en el 337D no el acceso sino la toma de posesión de una computadora, sistema informático, red informática o suministros informáticos. Así pues, ordenador significa un dispositivo electrónico que realiza funciones lógicas, aritméticas y de memoria mediante la manipulación de impulsos electrónicos o magnéticos, e incluye todas las instalaciones de entrada, salida, procesamiento, almacenamiento, software y comunicaciones que están conectados o relacionados con una computadora en un sistema informático o red de computadoras; sistema informático significa un conjunto interrelacionado de equipamiento informático hardware y software; finalmente, el sistema de información consiste en un dispositivo o grupo de dispositivos interconectados o relacionados, uno o más de los cuales, de acuerdo con un programa, procesa automáticamente los datos informáticos, así como los datos informáticos almacenados, procesados, recuperados o transmitidos por ese dispositivo o grupo de dispositivos para los efectos de su o su funcionamiento, uso, protección y mantenimiento.

[165] **MONTENEGRO.** El artículo 353 del Código penal de la República de Moldavia castiga el acceso al sistema informático, cuya definición recoge el ítem (16) del artículo 142 del Código: dispositivo o grupo de dispositivos mutuamente conectados o condicionados, de los cuales uno o varios, dependiendo del un programa, realizan el tratamiento automático de datos. De hecho, dicha norma es una de las más completas, pues recoge todas los conceptos previstos en el Convenio.

[166], Romania[167], Serbia[168] y la República de Macedonia[169]. Asimismo, unos pocos países han definido todos y cada uno de los términos propuestos en la Convención, pudiendo citarse como ejemplo Chipre[170], Bulgaria[171], o Sri Lanka[172].

De los países que sólo se protegen los datos informáticos y no el sistema en sí mismo, no todos ofrecen una definición de los

---

[166] **PORTUGAL.** Portugal tiene una de las regulaciones más completas y punteras en materia de ciberdelincuencia. Ya el artículo 7 de la Ley nº 109/1991, de 17 de agosto, de delitos relacionados con la informática recogió el delito de acceso ilícito a un sistema o a una red informáticos. Esta norma fue derogada por el artículo 6 de la Ley 109/2009, de 15 de septiembre, sobre el Delito Cibernético, que castiga en el artículo 6 dicha conducta conceptuando en el artículo 2 el sistema informático como cualquier dispositivo o conjunto de dispositivos interconectados o asociados, en que uno o varios de ellos desarrolla, ejecutando un programa, el tratamiento automatizado de datos informáticos, así como la red que soporta ésta comunicación entre ellos y el conjunto de datos informáticos almacenados, tratados, recuperados o transmitidos por aquel o aquellos dispositivos con vistas a su funcionamiento, utilización, protección y mantenimiento.

[167] **RUMANIA.** El artículo 181 del Código penal rumano define el concepto de sistema informático, objeto material del delito de acceso ilícito previsto en el artículo 360, como cualquier dispositivo o grupo de dispositivos (funcionalmente) interconectados, cuando uno o varios de estos sistemas aseguran tratamiento automatizado de datos, utilizando un programa de ordenador.

[168] **SERBIA.** El artículo 112 del Código penal de la República de Serbia define sistema informático como dispositivo o grupo de unidades interconectadas o dependientes de las cuales uno o más, basado en programa, el tratamiento automático de datos. El sistema informático será adoptado como objeto material del acceso en el artículo 302.

[169] **REPÚBLICA DE MACEDONIA.** El artículo 122 ítem (26) define sistema informático como todo dispositivo o un grupo de dispositivos interconectados, de los cuales, uno o varios de ellos, realizan el tratamiento automático de datos, de acuerdo con un programa, mientras que el artículo 251 (2) recoge la conducta de acceso.

[170] Artículo 2 de la Ley nº 22 (III) 04

[171] Artículo 93, ítems 21 a 23 del Código penal y Sección 1(2) del Código de Procedimiento penal

[172] El artículo 35 de la Ley nº 161/2003, define no sólo sistema informático y datos informáticos, sino también programa informático, medidas de seguridad, procesamiento automático de datos, y la expresión sin derecho. Artículo 38 de la Computer Crime Act nº 24/2007.

mismos. Entre ellos se encuentran Alemania[173], Australia[174],

[173] **ALEMANIA.** La § 202a (2) StGb afirma que los únicos datos protegidos en el delito de piratería informática o espionaje de datos son aquellos que se almacenan o trasmiten en forma electrónica, magnética, o de otra manera en forma no inmediatamente perceptible: *Daten im Sinne des Absatzes 1 sind nur solche, die elektronisch, magnetisch oder sonst nicht unmittelbar wahrnehmbar gespeichert sind oder übermittelt werden.* La definición que ofrece el Código penal alemán es considerada por el Informe del Consejo de Europa *National legislation implmenting the Convention on Cybercrime - Comparative analysis and good practices* excesivamente restringida que la recogida en el propio Convenio, puesto que incluso se excluye la noción de programa informático. Este bache con el que se encuentra la legislación alemana vendría a ser salvado en nuestra legislación con la alusión expresa al concepto de programa informático que efectuaba el hoy ya no vigente apartado 3 del artículo 197 del Código penal, de cuyo tenor literal se desprende que nuestro Código sigue la tónica del Código penal alemán a la hora de considerar algo distinto datos informáticos y programas informáticos -algo totalmente coherente desde mi punto de vista como más tarde se verá-. Sin embargo, la recomendación del Informe se centra en la introducción también de la definición de sistema informático, proveedor de servicios y tráfico de datos PICOTTI y SALVADORI, 2008: 11 y 12..

[174] **AUSTRALIA**. La Sección 476.1 y .2 del Código penal australiano también hacen referencia al acceso a datos contenidos en un ordenador. No obstante, en lugar de definir directamente lo que debe entenderse por datos informáticos, explica qué debe entenderse por dicho acceso: la visualización de los datos o cualquier *output* de éstos en el ordenador, copia o transferencia de los mismos a otro lado del ordenador o de un dispositivo de almacenamiento de datos o, en el caso de los programas informáticos, la ejecución de un programa en el caso de éste. De ello se desprende que, el Estado australiano incluye dentro del concepto de dato el de programa. Sí existió en el Código penal australiano una definición general de datos y de datos informáticos, introducida posteriormente en el Código penal a través de la *Cybercrime Act* de 2001, cuyas modificaciones han sido hoy parcialmente derogadas en el Código penal, entre ellas la relativa a la definición datos y datos contenidos en un ordenador, que nuevamente vuelven sólo a estar incluidos en la norma de procedencia de donde, de hecho, las definiciones fueron literalmente copiadas para traspasarlas al Código penal: la *Australian Security Intelligence Organisation Act* de 1979. Conforme a la redacción vigente desde el 25 de marzo de 2015, el artículo 22 de dicha última norma afirma, en este sentido, que el concepto general de dato englobará información, un programa informático o parte de éste. Tampoco aparece en el Código penal la definición de datos contenidos en un ordenador como aquellos datos contenidos en cualquier dispositivo de almacenamiento de datos removible por el tiempo que está éste contenido en el ordenador, así como aquellos datos contenidos en un dispositivo de almacenamiento de datos o en una red de ordenadores de la cual un ordenador forma parte.

Bulgaria[175], Dinamarca[176], [177], Grecia[178], Islandia[179], Malta[180],

[175] **BULGARIA.** El artículo 319 a del Código penal búlgaro protege también únicamente los datos informáticos, estableciendo un precepto agravado en el párrafo (4) cuando se trate de información que ha sido calificada de Secreto de Estado o protegida por la Ley. El artículo 93 ítem 22 define datos computarizados como cualquier representación de hechos, información o conceptos de una forma adecuada para su tratamiento automatizado, incluyendo programas de ordenador.

[176] **DINAMARCA.** La Sección 263 párrafo 2 no tiene como objeto material el sistema informático, sino que castiga el acceso a la información y a los programas contenidos en el sistema de información.

[177] **GEORGIA.** En artículo 284 del Código de Georgia no castiga el acceso a datos sino el acceso al sistema sino el acceso a la información contenida en el sistema

[178] **GRECIA.** Aunque con carácter general el artículo 370Γ ΠΚ castiga el acceso a datos grabados en un ordenador, sus memorias externas o transmitidos durante una telecomunicación, no es este precepto el que hace específica referencia a datos y programas informáticos (con independencia de que creo que ello puede desprenderse de una interpretación implícita). Así pues, es el artículo 370B ΠΚ párrafo 1 ofrece protección a los datos y programas informáticos siempre que estos contengan secretos de Estado o sean relativos a la privacidad de las personas, a secretos de empresa y a secretos comerciales y los párrafos 2 y 3 agravan las conductas dirigidas contra datos con un especial valor económico, relativos a secretos militares, diplomáticos o de la seguridad del Estado. La legislación griega mantiene, como puede observarse, el concepto de programa y de dato como nociones diferenciadas, pero, no obstante, adopta como eje central de la protección penal que éstos se hallen enmarcados dentro de la esfera de la privacidad. En este sentido, dicho precepto define in fine datos o programas informáticos de carácter privado como todos aquellos datos y programas que el titular mantiene secretos en virtud de un interés justificado, especialmente cuando éste ha adoptado medidas de seguridad.

[179] **ISLANDIA.** La Sección 1 del artículo 228 no tutela el acceso al sistema informático, sino a los datos y programas informáticos almacenados como datos

[180] **MALTA.** En el Código penal maltés el artículo 337B (1) tiene como objeto material del delito los datos, el software y la documentación de soporte. Dicho precepto recoge entre la amplia lista de definiciones entre las que se encuentran las de datos informáticos como cualquier representación de hechos, información o conceptos en una forma adecuada para su procesamiento en un sistema de información o en un sistema informático, incluido un programa adecuado para hacer que un sistema informático para realizar una función; software informático o software, esto es, un programa de ordenador, procedimiento o documentación asociada utilizada en la operación de un sistema informático; y documentación justificativa, que significa cualquier documentación utilizada en el sistema informático en la construcción, la aclaración, la aplicación, uso o modificación del software o los datos.

[181] y Noruega[182]. Finalmente, algunos países protegen tanto el acceso a los datos como el acceso al sistema. Este el caso de Bélgica[183],

[181] **MOLDAVIA.** El artículo 259 del Código penal moldavo adopta como objeto material del delito el concepto de información, entendiendo englobados dentro de éste los datos informáticos, los dispositivos de almacenamiento de datos, los sistemas informáticos y las redes informáticas.

[182] **NORUEGA.** La Sección 145 y 145 b del Código penal noruego no castiga, de hecho, el acceso al sistema, sino el acceso a los datos o al software.

[183] **BÉLGICA.** Aunque el Código penal de Bélgica recoge en el artículo 550 *bis* el acceso ilícito a un sistema informático, hace referencia en el párrafo 1º de su Sección 3 a los datos informáticos, castigando a quien, de alguna manera se apodere de datos almacenados, procesados o transmitidos por el sistema informático. En primer lugar cabe tomar como punto de partida las definiciones ofrecidas por la normativa internacional así como por otros países en la materia. No ofrece, sin embargo, una definición de lo que debe entenderse por dato informático.

Bosnia y Herzegovina[184], Croacia[185], Finlandia[186].

[184] **BOSNIA Y HERZEGOVINA.** Tanto el Código penal de la Republika Srpska como el de Brčko District en Bosnia y Herzegovina también castigan tanto el acceso al sistema como a los datos contenidos en él. Distinguen, además, los programas de los datos informáticos, el primero en el artículo 238 y 292 d y el segundo en los artículos 387 y 391 de sus respectivos Códigos penales. El artículo 238 del Código penal de la Republika Srpska tiene como objeto, de hecho, proteger el acceso y uso bases de datos informáticas y programas informáticos. No obstante, el Código de Procedimiento Penal de Bosnia y Herzegovina también recoge en su artículo 20 la definición de datos informáticos. Así, afirma que se trata de denota cualquier presentación de hechos, información o conceptos en una forma adecuada para su procesamiento por un sistema informático, incluyendo cualquier programa que es capaz de hacer que el sistema informático para ejecutar determinada función

[185] **CROACIA.** El artículo 266 párrafo (1) del Código penal de Croacia tutela tanto el acceso a datos como el acceso al sistema informático y, si bien, como se verá más adelante, integra dentro de la definición de sistema informático a los propios datos, incluye en el ítem (18) del artículo 87 una definición de éstos como cualquier representación de hechos, información o conceptos en una forma adecuada para su transformación en un sistema informático. Además, el ítem (19) también conceptúa qué debe entenderse por programa informático, esto es, un conjunto de datos informáticos adecuados para causar un sistema informático para realizar una función. El Código penal de Croacia pone el acento, pues, en los datos informáticos, ya que toma a éstos como base para la definición los conceptos de sistema y de programa informático, el cual, entiendo, debe entenderse protegido al amparo de tal expresión. El artículo 266 adopta, en este sentido, como objeto material al tipificar el acceso ilícito el sistema y los datos informáticos.

[186] **FINLANDIA.** El Código penal finlandés ofrece en la Sección 8 del Capítulo 38 del Código protección tanto al sistema como a los datos contenidos en él, si bien alude a ellos bajo el concepto información. No obstante, la protección de la información es mucho mayor porque no se exige la creación de una brecha en las medidas de seguridad, a diferencia de lo que el tipo penal exige para el sistema.

CAPITULO II

EL TRATAMIENTO PENAL DEL ACCESO ILÍCITO EN EL DERECHO COMPARADO

I. INTRODUCCIÓN

En el Capítulo anterior se han estudiado los distintos instrumentos de carácter supranacional que han conducido a la tipificación del acceso ilícito a un sistema informático en las distintas normativas nacionales, las cuales, además, han sido tratadas en el último apartado del mismo.

No obstante lo anterior, cabe resaltar que en algunos Estados (entre los que no se encuentra España) la tradición incriminatoria en materia de delincuencia informática y más especialmente por lo que respecta el delito objeto de estudio tiene más de dos décadas. Esta es la razón por la que el análisis de la evolución legislativa, jurisprudencial y doctrinal de la conducta de acceso ilícito en estos países resulta de extrema utilidad a los efectos del presente estudio.

El examen de estos aspectos permitirá situar el marco de trabajo e introducir algunas de las cuestiones que serán analizadas de forma pormenorizada en un estadio posterior. Este examen adquiere relevancia en la medida en que se presenta de forma global para cada país, pudiendo el lector obtener una rápida disección de la estructura del tipo penal, el cual será presentado en capítulos posteriores de forma fragmentaria y en atención a las propias necesidades expositivas.

Lo anterior permitirá no solo ofrecer una primera aproximación global a cada regulación nacional del acceso ilícito en su conjunto, necesaria para la presentación posterior del contenido, sino también una mejor comprensión de las conclusiones a las que se pretende llegar en el presente trabajo. De este modo, podrán extraerse las características típicas del acceso y los aspectos que los diferentes Estados han modificado para adaptar su normativa penal a las disposiciones supranacionales, así como estudiar cuál ha sido la problemática que se ha suscitado en torno a la redacción, interpretación y aplicación del tipo por parte de la doctrina y la jurisprudencia.

Específicamente, de entre los Estados tratados en el capítulo anterior se han seleccionado tres países:

a) En primer lugar, Alemania, porque ha sido uno de los países pioneros en la incriminación del acceso ilícito y porque la regulación que ha aprobado, recogida en la § 202a del Código penal alemán, guarda importantes similitudes con la primera redacción del tipo en el Código penal español introducido por la Ley Orgánica 5/2010, de 22 de junio.

b) En segundo lugar, Italia, un país cuya pionera regulación ha sido la que más ha influido en las dos descripciones típicas de las que ha gozado el precepto español relativo al acceso ilícito (la primera, conforme a la citada Ley Orgánica 5/2010, de 22 de junio y, la segunda, de acuerdo a la Ley Orgánica 1/2015, de 30 de marzo).

c) En tercer y último lugar, se realizará un breve estudio de la normativa vigente en Estados Unidos de América, la cual constituye el origen de ciertos aspectos de la redacción típica de los países a los que se ha hecho referencia y, por ende, de España.

II. ALEMANIA

A) MARCO NORMATIVO

En Alemania el acceso ilícito a un sistema informático se encuentra recogido en la § 202a del Código penal alemán bajo la rúbrica de espionaje de datos (*Ausspähen von Daten*). Dicho precepto fue introducido por la *2. Gesetz zur Bekämpfung der Wirtschaftskriminalität* (Ley contra la delincuencia económica) de 14 de mayo de 1986, que pretendía luchar contra la ciberdelincuencia y la delincuencia contra los datos. Sin embargo, en la redacción primigenia del precepto la conducta iba orientada a la protección directa de los datos, de modo que no podían quedar subsumidas en él las conductas de mero acceso al sistema[1]. Así se puso de manifiesto, de hecho, en la BT-DRUCKS 10/50058 de 1986[2].

Con la finalidad de adaptar dicha norma al Convenio sobre Cibercriminalidad de Budapest el 23 de noviembre de 2001 y a la Decisión Marco 2005/222/JAI, de 24 de febrero de 2005, relativa a los ataques a sistemas de información, dicho precepto fue modificado por la *41 Strafrechtsänderungsgesetz zur Bekämpfung der Computerkriminalität* de 2007 (Ley de lucha contra la delincuencia informática), permitiendo subsumir en ella el acceso ilícito a un sistema informático.

---

[1] GRAF, 2012: 179 párrafo 5.

[2] Drucksache 10/5058, 1986: 29.

B) LITERALIDAD DEL PRECEPTO

El acceso ilícito a un sistema informático aparece formulado en la § 202a del Código penal alemán como la conducta de *quien se procure para sí o para otro el acceso a datos que no le estén destinados y que estén particularmente protegidos contra un acceso ilícito, que se consigna con la vulneración de un acceso de seguridad*. En el párrafo 2º de la misma sección, el Código penal alemán define el concepto de datos: *únicamente aquellos que se hallan almacenados o son transmitidos electrónica, magnéticamente o de otra forma no perceptible directamente*[3].

Al amparo de esta redacción se distinguen desde 2007[4] dos modalidades típicas: procurarse datos (*Verschaffen von Daten*) y procurarse el acceso a los datos (*Verschaffen des Zugangs zu Daten*)[5], que serán tratadas con mayor detenimiento en los apartados siguientes.

---

[3] *§ 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.

[4] Hasta 2007 el tenor literal de la Sección 202a no se refería a procurarse el acceso a datos sino a procurarse los propios datos. Esta redacción fue modificada por la Sección 41. de la Ley StÄG v. 7.8.2007 (BGBl. I 1786), *Rechtswidriger Zugang su Informationssystemen* como consecuencia de la ratificación por Alemania del Convenio sobre Ciberdelcuencia de Budapest de 2001 y de la aprobación de la Decisión Marco 222/2005/JAI, de 22 de febrero, relativa a los ataques a sistemas de información, con motivo de incluir el mero acceso ilegal a sistemas informáticos. No obstante, puesto que el legislador alemán ha centrado el objeto material en los datos informáticos y no en el sistema, el Informe del Consejo de Europa ha criticado lo que considera una excesiva restricción de la conducta típica, entendiendo que Alemania no se adapta a las exigencias del Convenio. Véase Apartado X del Capítulo I.

[5] GRAF, 2012: 196 párrafo 49.

C) BIEN JURÍDICO PROTEGIDO

El bien jurídico protegido en el delito no es una cuestión clara. En origen el espionaje de datos fue concebido como un delito de naturaleza patrimonial, naturaleza que, por supuesto, condicionaba el bien jurídico[6]. Posteriormente, la ampliación del ámbito de tutela a la protección de todo género de datos ha llevado a la doctrina a centrarse en el derecho a la confidencialidad[7], y, desde la reforma de 2007, en el poder de disposición sobre éstos[8]. Actualmente, algunas voces apuntan igualmente a la integridad del propio sistema informático[9] y al secreto de las comunicaciones como bien jurídico protegido en el delito, en la medida en que también se ofrece protección a los datos que están en proceso de transmisión[10].

---

[6] Algunos autores consideraban que la protección debía limitarse a la protección de los datos que tuvieran algún genero de valor económico. SIEBER redactó la primera monografía sobre delincuencia informática en 1977. BÜHLER, 1987: 452. HAFT, 1987: 9. SIEBER, 1977: 98.

[7] Se considera que el bien jurídico no se proyecta sobre la propiedad del sistema, del medio de almacenamiento o del dispositivo de datos, así como tampoco sobre la esfera del sujeto, puesto que los datos contenidos en el sistema pueden tener diferente naturaleza. Por consiguiente, el bien jurídico se centra ahora en el derecho formal a la confidencialidad sobre los datos, entendido éste como derecho al contenido intelectual sobre datos que son trasmitidos o almacenados siempre y cuando tales datos se hallen protegidos contra el acceso no autorizado. ALTENHAIN y WIETZ, 2013: 1588 párrafo 1. DIETRICH, 2009: 27-59. DIETRICH, 2011: 247. ERNST, 2007: 2661. GRAF, 2012: 178 párrafo 2. HEGER, 2014: párrafo 1. HERZOG, 2009: 1-10. HILGENDORF, 2005: 49. HILGENDORF, 2012: 160-161. JESSEN, 1994: 37. KINDHÄUSER, 2013: 744 párrafo 1. LENCKNER y EISELE, 2010: párrafo 1. SCHMITZ, 1995: 478. SCHULZE-HEIMING, 1995: 37. SCHUMANN, 2007: 676.

[8] Al tener en cuenta que lo protegido son datos informáticos sobre los que se ha dispuesto una protección determinada, con independencia de su contenido. BOSCH, 2014: 1275 párrafo 1. FISCHER, 2013: 1359 párrafo 2. HOYER, 2012b: 2 párrafo 1. GRAF, 2012: 2. JOECKS, 2012: 351 párrafo 1. KARGL, 2013: 1406 párrafo 3. LENCKNER y EISELE, 2010: 2.

[9] ALTENHAIN y WIETZ, 2013: 1588 párrafo 1. BT-Drucks 16/3656, 2006: 7-9. GRÖSELING y HÖFINGER, 2007: 551. SIEBER, 2012: C 43.

[10] ALTENHAIN y WIETZ, 2013: 1588 párrafo 1.

Por lo que se respecta a la forma de afectación del bien jurídico, existe mayor acuerdo —casi unanimidad— en la literatura jurídica alemana en cuanto a considerar como un delito de lesión la modalidad de proporcionar la entrada a los datos y como un delito de peligro[11] abstracto[12] el acceso ilícito.

D) OBJETO MATERIAL DEL DELITO

El objeto material del delito son los datos informáticos. Como he indicado con anterioridad, la § 202a (2) acalra qué debe entenderse como tales a los efectos de la aplicación del precepto: *únicamente aquellos que se hallan almacenados o son transmitidos electrónica, magnéticamente o de otra forma no perceptible directamente*. En relación con esta definición, considera en general la doctrina que se trata de una noción muy abierta[13] y centrada en el concepto de información, ya que las únicas características que definen a tales datos son: ser ajenos al sujeto activo, ser o estar siendo transmitidos o almacenados de una forma no directamente perceptible y estar protegidos[14].

Los distintos términos que componen dicha definición son desglosados por la doctrina alemana del siguiente modo:

---

[11] GRAF, 2012: 178 párrafo 3.

[12] FISCHER, 2013: 1401 párrafo 2.

[13] La doctrina alemana ha puesto de manifiesto que se trata de un concepto difícil de delimitar en cuanto a contenido y que tropieza con el de datos personales. En este sentido, han sido múltiples las definiciones que los autores han propuesto con el fin de concretarlo. Uno de los pioneros en definir este concepto fue HAFT, quien entendió que el concepto de datos hace referencia a la información codificada en un sistema que se encuentra fuera de los caracteres utilizados en la realidad. HAFT, 1987: 6-8. ALTENHAIN y WIETZ, 2013: 1588 o párrafo 2. FISCHER, 2015: página 1395 o párrafo 2. GRAF, 2012: 181 o párrafo 12. HILGENDORF, 2005: 1442 o párrafo 7. HOYER, 2012b: 3 o párrafo 3 (Abschnitt 15). KARGL, 2013: 1407 o párrafo 4. KINDHÄUSER, 2013: 1819. HEGER, 2014: 965 o párrafo 2.. SCHÖNKE y SCHRÖDER, 2010: 1820. TAG, 2013: 1091 o párrafo 4. WEIDEMANN, 2010: 1307 o párrafo 4.

[14] Esta característica se estudiará en el correspondiente apartado relativo a los elementos objetivos de la conducta.

a) Almacenamiento: es el registro, incorporación o grabación de los datos en un soporte o dispositivo digital o analógico de cualquier tipo[15], con el propósito de su conservación, procesamiento y/o uso posterior[16].

b) Transmisión: es la transferencia a través de la conexión a una red de área local o de telecomunicaciones por vía electrónica o no corporal hacia una localización diferente de datos almacenados u objeto de procesamiento a los efectos de ponerlos a disposición del examen de o acceso a los mismos por parte de un tercero[17].

c) Ausencia de percepción directa: significa que sólo se protegen aquellos datos cuyo acceso a la percepción sensorial puede producirse únicamente mediante la utilización de dispositivos técnicos que permitan la transformación o ampliación de los mismos por parte de una persona media[18]. Ello implica, asimismo, la existencia de algún tipo de transformación técnica de los datos por

---

[15] Así como la naturaleza y formato del soporte es irrelevante se afirma que la idoneidad como objeto del delito se mantendrá únicamente cuando el almacenamiento continúe. ALTENHAIN y WIETZ, 2013: o párrafo 2. FISCHER, 2015: página 1396 o párrafo 5. HILGENDORF, 2005: 67 o párrafo 13. WEIDEMANN, 2010: 1307 o párrafo 5.

[16] BOSCH, 2014: 1276 o párrafo 3. FISCHER, 2015: página 1396 o párrafo 5. GRAF, 2012: 183 o párrafo 18. HOYER, 2012a: 3 o párrafo 4 (Abschnitt 15). KARGL, 2013: 1407 o párrafo 6.

[17] Quedan excluidos de la definición los datos que todavía no se han introducido (*input data*) y los datos que ya han sido enviados (*output data*). ALTENHAIN y WIETZ, 2013: o párrafo 2. BOSCH, 2014: 1276 o párrafo 3. FISCHER, 2015: página 1396 o párrafo 6. GRAF, 2012: 183 o párrafo 18. KARGL, 2013: 1407 o párrafo 6. HOYER, 2012a: 3 o párrafo 4 (Abschnitt 15). SCHÖNKE y SCHRÖDER, 2010: 1819. WEIDEMANN, 2010: 1307 o párrafo 4.

[18] GRAF, 2012: 181 o párrafo 13. HILGENDORF, 2005: 1442 o párrafo 11. HOYER, 2012a: 3 o párrafo 4 (Abschnitt 15). KARGL, 2013: 1407 o párrafo 5. KINDHÄUSER, 2013: 764. SCHÖNKE y SCHRÖDER, 2010: 1819. WEIDEMANN, 2010: 1307 o párrafo 4.

cualquier medio, aunque la doctrina no distingue qué tipo de tecnología debe haberse utilizado para ello[19].

d) Datos protegidos: los datos en la § 202a (2) StGb son solo aquellos transmitidos o almacenados de una forma no directamente perceptible, esto es, que se trate de información codificada[20] por hallarse registrados, o bien que se hallen almacenados de una forma no directamente perceptible o bien porque se encuentran siendo transmitidos de una forma no directamente perceptible[21].

Además de señalar la vaguedad de la definición, la doctrina alemana ha sido muy crítica con la misma y le ha atribuido un valor muy escaso. Dos son los principales puntos de crítica:

a) Excesiva generalidad: En primer lugar, se aduce que se trata de una enunciación genérica que resulta aplicable a cualquier ámbito del Derecho sin que aporte nada en particular a la descripción penal del tipo[22]. De este modo, se considera que no es posible identificar cuáles son los datos a los que se ofrece protección, ya que la noción legal de dato no aparece claramente delimitada de una manera positiva sino únicamente a través de la limitación del concepto por medio de la exigencia de características adicionales[23].

---

[19] FISCHER, 2015: página 1396 o párrafo 4. GRAF, 2012: 181 o párrafo 12.

[20] ALTENHAIN y WIETZ, 2013: 1588 o párrafo 2. FISCHER, 2015: página 1396 o párrafo 4.. HEGER, 2014: 965 o párrafo 2. HILGENDORF, 2005: 1442 o párrafo 10.

[21] BOSCH, 2014: 1275 o párrafo 2. HILGENDORF, 2005: 1442 o párrafo 10.

[22] BOSCH, 2014: 1275 o párrafo 2. KARGL, 2013: 1407 o párrafo 4.

[23] El único aspecto positivo que la doctrina alemana concibe en la definición es su apertura a los nuevos avances de la tecnología. Parece, pues, que el legislador alemán, aún habiendo ido un paso más allá que el español al pretender positivizar el concepto de datos informáticos, en realidad ha cometido los mismos errores que éste a la hora de configurar el concepto de datos informáticos, que adolece de las mismas deficiencias que el artículo 197.3: excesiva generalidad y delimitación mediante una interpretación de carácter negativo. ALTENHAIN y WIETZ, 2013: 1588 o párrafo 2. GRAF, 2012: 180-181 o párrafo 10. KARGL, 2013: 1407 o párrafo 4. TAG, 2013: 1091 o párrafo 4.

Tratando de evitar que dentro del concepto de datos *ex* § 202a (2) queden englobados todo tipo de datos[24] y de cualquier formato[25], algunos autores han intentado adaptar el concepto previsto en dicha Sección estableciendo algunas limitaciones interpretativas. Así, una suerte de restricción en atención al bien jurídico realizan KARGL, para quien solo pueden caer en la esfera de la § 202a (2) datos con un interés legítimo para el uso y el conocimiento del propietario, y GRAF, al defender que, aunque la formulación del apartado 1 habla de datos en general, debe tratarse de datos protegidos contra el espionaje[26].

b) Vinculación directa el concepto de información: en segundo lugar, se afirma también que la noción de dato se centra excesivamente en el concepto de información. De este modo, éste se define como una representación de la información que es susceptible de ser entendida a través de códigos definidos con independencia de que esté dirigida a fines de procesamiento[27].

---

[24] A diferencia de lo que sucede en el ámbito español, donde esta interpretación atentaría contra el bien jurídico, en la noción de datos de la § 202a (2) StGb son susceptibles, según la doctrina, de ser englobados no solo los datos personales o secretos sino también aquellos que son de libre acceso, por ejemplo, en Internet. Además, tales datos no tienen por qué ir necesariamente referidos a datos individuales sobre las relaciones personales y objetivas, sino que pueden ser de cualquier clase: compilaciones, de conocimiento científico, documentación o resultados de cálculo. También incluye datos que no tienen ningún valor económico, científico o sentimental. ALTENHAIN y WIETZ, 2013: o párrafo 2.. BOSCH, 2014: 1275 o párrafo 2. FISCHER, 2015: página 1395 o párrafo 2. GRAF, 2012: 180-181 o párrafo 10. HEGER, 2014: 965 o párrafo 2. HILGENDORF, 2005: 1442 o párrafo 8.

[25] Tanto música, vídeo o películas, como otro tipo de datos digitales. KARGL, 2013: 1407 o párrafo 4.

[26] GRAF, 2012: 180-181 o párrafo 10.

[27] HOYER, 2012a: 3 o párrafo 3 (Abschnitt 15). GRAF, 2012: 180-181 o párrafo 10. KARGL, 2013: 1407 o párrafo 4. WEIDEMANN, 2010: 1306 o párrafo 3.

También ha sido criticada esta definición —y la fijación de los datos informáticos como objeto material del delito— desde la perspectiva internacional. Concretamente, la § 202a (2) ha sido analizada por varios expertos del Consejo de Europa en materia de delincuencia informática a través del Informe *National legislation implementing the Convention on Cybercrime - Comparative analysis and good practices.* De acuerdo con las conclusiones a las que han llegado tales expertos en dicho Informe, la § 202a del Código penal alemán no se adapta a las exigencias del Convenio de Budapest sobre Cibercriminalidad de 23 de noviembre de 2001[28]. En este sentido, a la misma conclusión puede llegarse por lo que se refiere a la Directiva 2013/40/UE del Parlamento Europeo y del Consejo, de 12 de agosto de 2013, relativa a los ataques contra sistemas de información.

---

[28] Las **razones** que se pueden alegar para afirmar la incorrecta adaptación de la regulación alemana a las exigencias de la normativa supranacional son dos:

> a) Por una parte, el objeto material del delito de acceso ilícito no son los datos sino el sistema.
>
> b) Por otra parte, la § 202a (2) del Código penal alemán restringe en demasía la noción de dato informático prevista en la normativa supranacional debido a que la noción supranacional de dato es más abierta, entendiendo englobada cualquier representación (hechos, informaciones o conceptos) susceptible de procesamiento automatizado, ya que ninguna de las dos normas enunciadas hace referencia a las abstractas restricciones a las que el Código penal alemán ha sometido dicho concepto, especialmente la ausencia de perceptibilidad, lo que conduce a dejar fuera del ámbito típico todo un conjunto de datos que también deberían ser considerados informáticos. Desde esta perspectiva, la restricción del concepto de dato no parece adecuada.
>
> PICOTTI y SALVADORI, 2008: 16.

E) MODALIDADES TÍPICAS

La conducta típica viene determinada por la acción de procurarse para sí (*verschaffen*). La doctrina alemana define de un modo genérico esta acción como el acto de proporcionarse para sí o para un tercero datos informáticos o un soporte que contenga tales datos[29]. Además, el Código penal alemán divide alternativamente en dos las modalidades típicas de esta conducta:

1. APODERAMIENTO DE LOS DATOS CONTENIDOS EN EL SISTEMA INFORMÁTICO: *VERSCHAFFEN VON DATEN*

El apoderamiento de los datos implica la efectiva adquisición por parte del sujeto activo de la posesión de éstos, lo que puede tener lugar a través de dos vías: o bien mediante la obtención material de los datos a través de la adquisición de la posesión sobre el dispositivo original de almacenamiento donde éstos se encuentran grabados, la realización de una copia del documento donde se encuentran contenidos mediante una máquina fotocopiadora, su traslado a otro dispositivo de almacenamiento, impresión, grabación, filmación o cualquier otra forma de obtención que permita poseerlos de forma física e inmediata; o bien mediante su obtención inmaterial a través del su conocimiento directo, lo que equivale a retenerlos mentalmente en la cabeza o escribirlos[30].

---

[29] ALTENHAIN y WIETZ, 2013: 1590.

[30] La opinión de los autores en relación con la admisión de una u otra forma de apropiación no es unánime. Se citan como ejemplo de esta conducta el fotocopiado, fotografiado o grabación en video de los datos, así como la realización de una captura de pantalla del monitor o su impresión. Se excluye, sin embargo, la apropiación de un papel impreso o la mera instalación de un programa. Igualmente, se excluye de este supuesto el acceso inicialmente autorizado, pero con apoderamiento ulterior en tanto extralimitación del acceso lícito *ab initio*. FISCHER, 2013: 1361 párrafo 10. GRAF, 2012: 196 párrafo 49; 197 párrafo 52. KARGL, 2013: 1413 párrafo 12. WEIDEMANN, 2010: 1309 párrafo 15.

La consumación de esta primera modalidad se produce cuando el autor o el tercero consigue lograr un verdadero control sobre los datos, entendido éste como un poder de disposición o disponibilidad sobre ellos tras la superación de las medidas de seguridad dispuestas para impedirlo[31]. Así, la disponibilidad sobre los datos se puede obtener bien mediante la superación de las medidas de seguridad o también mediante la averiguación subrepticia de las claves que permiten lograr el acceso a tales datos[32].

2. ACCESO A LOS DATOS: *VERSCHAFFEN DES ZUGANGS ZU DATEN*

La conducta de acceso a datos fue introducida en 2007 por medio de la reforma operada por la Ley StÄG v. 7.8.2007 (BGBl. I 1786), *Rechtswidriger Zugang su Informationssystemen*, a la que se ha hecho referencia anteriormente y que se aprobó con la finalidad de adaptar el contenido del Código penal alemán a las disposiciones del Convenio sobre Cibercrimen de 23 de noviembre de 2001. Abiertamente había sido reconocido tanto por la doctrina alemana como por el legislador alemán que el mero acceso a un sistema informático ajeno sin apoderamiento no podía ser subsumido en la § 202a del Código penal alemán[33] sin reformarlo. Sin embargo, su tipificación ha sido una cuestión polémica, pues a día de hoy la doctrina mayoritaria aboga por su derogación, aun aceptando que se trata de una imposición de carácter internacional[34].

---

[31] Dentro del tipo penal se prevé un esquema doble: por una parte, la posibilidad de que el autor directo del delito se procure para sí los datos, caso en el que sería él mismo a quien se le exigiera para la perfección del delito la obtención de un poder de disposición para entender perfeccionado el delito; por otra parte, es posible que el autor directo sólo consiga el soporte o los datos con la finalidad de entregárselo a un tercero, siendo que éste será quien obtiene el control sobre los datos o su conocimiento, manteniéndose la autoría del delito en el sujeto anterior. BOSCH, 2014: 1277 párrafo 6. GRAF, 2012: 197 párrafo 54. KARGL, 2013: 1413 párrafo 12. KINDHÄUSER, 2013: 746 párrafo 5. HEGER, 2014: 922 párrafo 5.

[32] GRAF, 2012: 197 párrafo 53. KARGL, 2013: 1413 párrafo 12.

[33] Drucksache 10/5058, 1986: 28.

[34] BOSCH, 2014: 1277 párrafo 7. FISCHER, 2013: 1361 párrafo 10.

Esta conducta se define como la acción de penetrar superando las medidas de seguridad impuestas para impedirlo en un dispositivo de almacenamiento de datos, un ordenador, una red o la línea de comunicación, ello con la finalidad de conseguir que el autor o un tercero se encuentre en la posibilidad de percibir el contenido del sistema informático o copiarlo[35].

La consumación del delito se produce cuando el sujeto ha superado las medidas de seguridad dispuestas para impedir el acceso a los datos informáticos, hecho que le otorga un contacto directo con los datos[36]. Para ello, no obstante, no es necesaria la obtención del contenido del soporte, la toma de conocimiento sobre los datos contenidos en él[37] o la alteración, destrucción o cesión a terceros de éstos[38]. La ausencia de tales exigencias ha llevado a la doctrina a afirmar la excesiva laxitud en la aplicación del tipo y a abogar por su derogación, ello sobre la base de que se trata de una conducta de inferior lesividad y que no puede ser equiparada a la de apoderamiento de datos, el auténtico espionaje[39], de una manifiesta mayor insidiosidad[40].

---

[35] ALTENHAIN y WIETZ, 2013: 1590 párrafo 7.

[36] BOSCH, 2014: 1277 párrafo 6.

[37] BOSCH, 2014: 1277 párrafo 6. GRAF, 2012: 197 párrafos 50-52. FISCHER, 2013: 1361 párrafo 11. KARGL, 2013: 1413 párrafo 12. KINDHÄUSER, 2013: 746 párrafo 5.

[38] BOSCH, 2014: 1277 párrafo 6. GRAF, 2012: 197 párrafos 50-52. FISCHER, 2013: 1361 párrafo 11. KARGL, 2013: 1413 párrafo 12. KINDHÄUSER, 2013: 746 párrafo 5.

[39] GRAF, 2012: 196 párrafo 51.

[40] FISCHER, 2013: 1361 párrafo 10.

F) ELEMENTOS DEL TIPO OBJETIVO

El Código penal alemán añade a la acción dos exigencias de carácter objetivo:

1. SIN AUTORIZACIÓN

Por una parte, la conducta debe llevarse a cabo en ausencia de autorización. Ésta es definida por la doctrina como el acceso a datos que han sido especialmente asegurados y que no están destinados para el sujeto[41]. A este efecto, la doctrina observa la existencia de una **relación directa entre la autorización y el poder de disposición** sobre los datos[42]. Así pues, los datos no serán disponibles para aquel que carece de autorización para acceder a los mismos, y a la inversa[43]. Lo mismo ocurre entre autorización y propiedad sobre los datos, en tanto en cuanto se califica a este delito como un delito especial de carácter negativo (*negatives Sonderdelikt*)[44] en el que el poder de autorización lo detenta quien ha realizado el acto de creación de los datos (*Skripturakt*), pudiendo éste quedarse la autoridad sobre los mismos o transferir el poder de acceso a otro[45]. No se observa esta relación, en cambio, entre autorización y propiedad sobre el dispositivo de almacenamiento o de tratamiento de datos, que resulta indiferente para determinar la existencia de autorización. De este modo, el propietario del dispositivo podrá considerarse como no autorizado a los efectos de la comisión del delito[46].

---

[41] En cambio, JESSEN proponía la eliminación de este elemento del tipo penal. JESSEN, 1994: 138. KARGL, 2013: 1412 párrafo 11.

[42] Los datos están destinados a aquél que ostenta una facultad de disposición sobre los mismos, porque ha sido quien los ha recogido y los ha guardado o porque están siendo transmitidos hacia su dispositivo de recepción de datos. GRAF, 2012: 184 párrafo 19.

[43] BOSCH, 2014: párrafo 5. FISCHER, 2013: párrafo 8. GRAF, 2012: 184 párrafo 20. HILGENDORF, 1996: 894. HOYER, 2012b: párrafo 7. KARGL, 2013: 1412 párrafo 11. LENCKNER y EISELE, 2010: párrafo 9. WEIDEMANN, 2010: párrafo 14.

[44] BOSCH, 2014: 1279 párrafo 11.

[45] HILGENDORF, 1996: 892. GRAF, 2012: 184 párrafo 20.

[46] SCHREIBAUER y HESSEL, 2007: 616. HILGENDORF, 2005: 512.

2. LA ESPECIAL PROTECCIÓN DE LOS DATOS

La § 202a exige también que los datos objeto del delito se hallen especialmente protegidos contra el acceso ilícito, de modo que el sujeto activo debe acceder a una zona protegida del sistema para entender configurable la infracción penal. La protección a la que hace referencia se concreta según la doctrina en el conjunto de medidas idóneas que el titular del derecho de autorización ha adoptado para dificultar el acceso a los datos y **expresar su interés** en que éste no se produzca[47]. En consecuencia, las medidas de seguridad se instituyen en el reflejo directo del bien jurídico protegido puesto que expresan el interés del titular del sistema en mantener el contenido de los datos de forma confidencial[48]. Es por esta razón que es necesario que los medios de seguridad adoptados sean siempre **idóneos para proteger** este interés de confidencialidad, asegurando los datos contra el acceso[49].

Esta idoneidad no se cifra para la doctrina en que la superación de las medidas de seguridad resulte más o menos difícil al sujeto activo, o en que éstas le sean perceptibles[50],

---

[47] ALTENHAIN y WIETZ, 2013: 1589 párrafo 6. HILGENDORF, 2012: 164 párrafo 546. HOYER, 2012b: párrafo 8. KARGL, 2013: 1410 párrafo 8. LENCKNER y EISELE, 2010: párrafo 6. Crítico con ello DIETRICH, 2011: 247, 250. SCHUHR, 2010: 155.

[48] GRAF, 2012: 190 párrafo 32.

[49] Se excluyen, sin embargo, aquellos medios que tienen otra finalidad los que tienen como función el mero aseguramiento de la prueba o el control empresarial tales como videocámaras o la mera entrada de un usuario, así como aquellos otros aparatos mecánicos que tienen como finalidad impedir el uso no autorizado del hardware o del dispositivo de almacenamiento de los datos. DIETRICH, 2011: 247, 250. GRAF, 2012: 190 párrafo 32.

[50] Para la literatura alemana lo importante es solo documentar que el sujeto activo ha tenido interés y conocía la existencia de la medida de seguridad que tenía que superar para poder acceder al los datos contenidos en el sistema, motivo por el cual caen dentro del campo de aplicación del precepto también las medidas que tengan un carácter oculto. BOSCH, 2014: 1276 párrafo 5. ERNST et al., 2004: 3233. FISCHER, 2013: 1360 párrafo 8-9. GRAF, 2012: 190 párrafo 32.

tampoco en la calidad de las medidas[51], ni en el tipo de éstas —incluye los medios técnicos o mecánicos tipo hardware como medios lógicos tipo software[52]—, la cantidad de los obstáculos a superar por quien desee ilícitamente acceder, o en una declaración expresa de confidencialidad de los datos por parte de su propietario, sino simplemente en que deben haberse adoptado las medidas adecuadas para garantizar de manera objetiva que queda patente la intención del titular de que conforme a su voluntad se pretende evitar el acceso a los mismos[53]. Es suficiente, por tanto, la **mera existencia** de la medida[54].

Se plantea la doctrina alemana si puede afirmarse su concurrencia cuando el acceso a los datos se produce por una persona no autorizada y a la que los datos no están destinados pero que dispone de acceso autorizado a las medidas de seguridad donde sistema donde estos se encuentran. Considera, a tal efecto, que los datos estaban asegurados contra el acceso[55].

---

[51] La medida no tiene por qué ser totalmente insuperable, porque en este caso la propia agresión no existiría. No obstante, se exige la disposición de una medida en cierta medida eficaz para el objetivo que pretende cumplir. Tampoco se exige que los datos deban ser especialmente asegurados cada vez contra del acceso no autorizado. BOSCH, 2014: 1276 párrafo 5. GRAF, 2012: 190 párrafo 32. HILGENDORF, 2012: 166 párrafo 554. KARGL, 2013: 1410 párrafo 10. LENCKNER y EISELE, 2010: 1821 párrafo 8.

[52] Dentro de los primeros se citan todos los dirigidos a salvaguardar físicamente los dispositivos de almacenamiento, huellas digitales, aparatos de reconocimiento de voz. Entre los segundos se hace referencia a las *passwords*, Firewall, ocultamiento de datos, esteganografía, medios de seguridad tridimensionales. ALTENHAIN y WIETZ, 2013: 1589 párrafo 6. DIETRICH, 2009: 179. ERNST et al., 2004: 3236. GRAF, 2012: párrafo 36. JESSEN, 1994: 154. KARGL, 2013: 1411. KRUTISCH, 2004: 112. LENCKNER y EISELE, 2010: 1821 párrafo 8. SCHUMANN, 2007: 676. TAG, 2013: 1092 párrafo 7. WEIDEMANN, 2010: 1308 párrafo 13.

[53] LENCKNER y EISELE, 2010: 1821 párrafo 8.

[54] GRAF, 2012: 190 párrafo 32. KARGL, 2013: 1410 párrafo 9.

[55] HILGENDORF, 2012: 166 párrafo 554.

G) TIPO SUBJETIVO

Desde un punto de vista subjetivo, se castiga únicamente la modalidad **dolosa** de la conducta, lo que supone que el sujeto activo debe conocer que ha obtenido los datos que no estaban destinados para él y que ha superado todos los obstáculos necesarios para lograr la entrada y obtener la disposición de éstos[56]. **No es necesaria**, además, la concurrencia de un **ánimo especifico ulterior** en la conducta del sujeto[57].

H) TRATAMIENTO DEL ERROR

Constituirán **error de tipo** aquellos supuestos en los que el autor se proporciona los datos creyendo que han sido destinados a él[58] o porque los datos no han sido asegurados[59] o porque la autorización de acceso ha sido revocada en el intermedio[60]. Por lo que respecta al **error de prohibición** tendrá lugar cuando el sujeto accede a datos creyendo que los mismos le afectan[61] o cuando cree que la revocación del poder de disposición es inefectiva[62].

---

[56] Admiten dolo eventutal FISCHER, HOYER y KINDHÄUSER FISCHER, 2013: 1361 párrafo 10. GRAF, 2012: 204 párrafo 71. HILGENDORF, 1996: 705. HOYER, 2012b: 7 párrafo 16. JESSEN, 1994: 146. KARGL, 2013: 1414 párrafo 15. KINDHÄUSER, 2013: 746 párrafo 9. SCHMID, 2001: 117. SCHULZE-HEIMING, 1995: 84.

[57] BOSCH, 2014: 1278 párrafo 8. FISCHER, 2013: 1361 párrafo 10. GRAF, 2012: 204 párrafo 71. KARGL, 2013: 1414 párrafo 15. LENCKNER y EISELE, 2010: 1823 párrafo 12.

[58] BOSCH, 2014: 1278 párrafo 8. HILGENDORF, 1996: 705. FISCHER, 2013: párrafo 13. KRUTISCH, 2004: 128. LENCKNER y EISELE, 2010: 1823 párrafo 12. TAG, 2013: 1093 párrafo 11. WEIDEMANN, 2010: 1311 párrafo 19.

[59] En contra, GRAF considera que el error sobre la existencia de las medidas de seguridad no es viable en la práctica, porque no es posible suponer que el sujeto activo desconocía que no estaba autorizado para el acceso y, por ello, ha sobrepasado tales medios dispuestos sobre los datos. GRAF, 2012: 204 párrafo 72. KARGL, 2013: 1414 párrafo 15.

[60] ALTENHAIN y WIETZ, 2013: 1591 párrafo 9. GRAF, 2012: 204 párrafo 72.

[61] FISCHER, 2013: párrafo 13. KARGL, 2013: 1414 párrafo 15. Detalladamente SCHULZE-HEIMING, 1995: 84.

[62] GRAF, 2012: 204 párrafo 72.

I) AUTORIA Y PARTICIPACIÓN

Desde el punto de vista del sujeto activo, el espionaje de datos se configura en Alemania como un **delito común**[63]. El autor es, por tanto, cualquiera a quien los datos no hayan sido destinados, lo que conduce a la doctrina a calificar a este delito como un **delito de especial de carácter negativo** (*negatives Sonderdelikt*)[64].

Aquel a quien los datos sí han sido destinados podría considerarse **partícipe** si le indica a otro como acceder a éstos facilitándole así la comisión del delito (complicidad)[65] o si, desconociendo como saltarse las medidas de seguridad, solicita a un tercero que lo haga para poder acceder a los datos (inducción)[66]. Especialmente se refiere la doctrina alemana a los supuestos en los que el sujeto tiene una posición de garante sobre el sistema que le obliga a garantizar la seguridad sobre los datos[67].

J) PENA

Los **actos preparatorios** del delito se castigan en la § 202c[68]. Además, es un **delito privado**, de forma que su persecución requiere denuncia previa (§ 205).

---

[63] ALTENHAIN y WIETZ, 2013: 1592 párrafo 11.

[64] BOSCH, 2014: 1279 párrafo 11.

[65] BOSCH, 2014: 1279 párrafo 11. FISCHER, 2013: 1363 párrafo 14.

[66] GRAF, 2012: 215 párrafo 99.

[67] BOSCH, 2014: 1279 párrafo 11.

[68] *§ 202c Vorbereiten des Ausspähens und Abfangens von Daten*

(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.

III. ITALIA

A) MARCO NORMATIVO

En el Código penal italiano el delito objeto de estudio fue introducido como un tipo penal autónomo a través del artículo 4 de la Ley 547/1993, de 21 de diciembre, sobre criminalidad informática. Con ello se dió aplicación a una de las previsiones contenidas en la Recomendación 89 (9), del Consejo de Europa, adoptada el 13 de septiembre de 1989, sobre delincuencia informática.

B) LITERALIDAD DE LA NORMA

La conducta fue introducida en el artículo 615 *ter*, en el seno de los delitos contra la inviolabilidad del domicilio. Este precepto sanciona desde entonces el delito de acceso abusivo a un sistema informático o telemático, que se describe como la conducta de introducirse abusivamente en un sistema informático o telemático protegido por medidas de seguridad o de mantenerse en él contra

la voluntad expresa o tácita de quien tiene un derecho de exclusión[69].

La conducta se ve, además, agravada por varias circunstancias: el perfil subjetivo del autor (el título de funcionario público o de representante de la administración pública o privada del sujeto activo), los medios comisivos de la acción (la violencia contra la propiedad o ejercida sobre las personas o la utilización de armas) y los resultados adicionales a la acción de acceder causados como consecuencia de la introducción del sujeto en el sistema (destrucción o daños en el sistema o la interrupción total o parcial de su funcionamiento o la destrucción o corrupción de datos, información o programas contenidos en él).

---

[69] *Art. 615-ter. Accesso abusivo ad un sistema informatico o telematico*

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 palesamente 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 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.

C) BIEN JURÍDICO PROTEGIDO

El bien jurídico protegido en el delito es una de las cuestiones más debatidas por la doctrina italiana y, como tal, está todavía hoy lejos el hallar una posición unánime entre los distintos autores[70].

A continuación se presentan las distintas posturas defendidas al respecto:

1. DOMICILIO INFORMÁTICO

a) EL DOMICILIO INFORMÁTICO COMO BIEN JURÍDICO

La peculiar ubicación sistemática del tipo entre los delitos contra la inviolabilidad del domicilio ha conducido a la mayor parte de la doctrina italiana a identificar el bien jurídico protegido con el **domicilio informático**[71]. Genéricamente, éste es susceptible de ser identificado con el espacio, manifestación del *ius excludendi* del titular, en el que se encuentran los datos informáticos pertenecientes a una persona, los cuales se protegen frente a cualquier tipo de intromisión no autorizada[72].

Dentro del sector de la doctrina que concibe el domicilio informático como el bien jurídico protegido en el delito, pueden distinguirse tres corrientes:

---

[70] CANNATA, 2006: 527.

[71] Se entendió que ello se debía a la más general exigencia de asegurar aquella simetría entre el viejo y el nuevo derecho en el punto de individualización de los bienes jurídicos protegidos, impuesta por la necesidad de dar autonomía sistemática a la nueva normativa dirigida a sistematizar las nuevas figuras informáticas en el Código penal. BERGHELLA y BLAIOTTA, 1995: 2329-2330.

[72] Relazione Ministeriale di accompagnamento alla legge n. 547/93, pág. 9. ALMA y PERRONI, 1997: 505. BORRUSO, 1994b: 28. CARINGELLA et al., 2011: 1051. CUOMO, 2000: 2998. CUOMO y RAZZANTE, 2009: 96. DESTITO et al., 2007: 81, 83. FIANDANCA y MUSCO, 2013: 293. GALDIERI, 1996: 189. GALDIERI, 1997: 138. GAROFOLI, 2013: 639. GATTA, 2011a: 300. MARANI, 2007: 613. MONACO, 2011: 2334. PARODI y CALICE, 2001: 64-65. PICA, 1999: 68. RELLA, 2007: 39.

a) Domicilio informático como expansión del domicilio tradicional: algunos autores consideran que los sistemas informáticos constituyen una expansión ideal del área de respeto perteneciente al sujeto interesado que aparece garantizada en el artículo 14 de la Constitución italiana y penalmente tutelada en sus aspectos más especiales y tradicionales en los artículos 614 y 615 del Código penal italiano[73].

b) Espacio informático: en cambio, otros autores hacen referencia —sin hacer una alusión directa al domicilio propiamente dicho pero en similares términos— al *espacio informático*, concibiendo a éste como el espacio inmaterial informático del que puede disponer libremente el sujeto sin intrusiones no deseadas[74]. La atención se centra desde esta perspectiva en una intrusión lesiva en el derecho que asiste al sujeto legitimado a acceder al ordenador y las informaciones contenidas en él[75]. La violación del domicilio informático sería punible sin que fuera necesario atacar el ámbito espacial en el cual materialmente se hayan colocados los dispositivos que integran el sistema informático, a causa de la naturaleza virtual del mecanismo de funcionamiento de los objetos de tratamiento de la información[76].

---

[73] Disegno di Legge n. 2773 citada en CANNATA, 2006: 521. También BORRUSO, 1994b: 28. GALDIERI, 1996: 189. DI GIANNANTONIO, 2001: 2029. LUBERTO, 2008: 898. PLANTAMURA, 2006b: 417. PLANTAMURA, 2006a: 847. PICA, 1999: 68. VANNINI, 1994: 427.

[74] Se afirma, pues, que el objeto del acceso abusivo no está vinculado al ámbito espacial en el sentido tradicional, que viene a caracterizarse por la invasión o el ingreso físico, el cual está indefectiblemente vinculado a la morada privada, a la habitación y a sus dependencias. CUOMO, 2000: 96. PICA, 1999: 68. PICOTTI, 2006: 335.

[75] Como se observa, la atención se dirige al derecho del titular a excluir a terceros de la esfera de disponibilidad y respeto creada y susceptible de aprovechamiento por parte de la tecnología informática. PETRINI, 2004: 43.

[76] CUOMO, 2000: 96.

c) Teoría mixta: Finalmente otros autores aúnan ambos aspectos, el físico y el ideal, y definen el domicilio informático como el espacio físico e ideal de pertenencia de la esfera individual personal tutelada en la Constitución[77].

Un punto común para los defensores de cualquiera de las tres tesis expuestas lo constituye el hecho de que la protección del sistema en aras a salvaguardar el domicilio informático resulta independiente de la tutela de su contenido[78]. Concretamente, estos autores consideran que el acceso ilícito conforma la anticipación de la tutela de la reserva de los datos y programas, especialmente los de carácter económico-patrimonial[79] y, por ello, lo califican como un delito de peligro abstracto[80] en el que el sujeto activo penetra en la memoria del sistema informático *invito domino* y se sitúa en la posición de conocer el contenido reservado del mismo[81].

Sin embargo, otros autores consideran que se trata de un delito de lesión, que se consuma en el momento de la intrusión y en el que no es necesario que se produzca algún daño para el sistema o interrupción de su funcionamiento[82].

---

[77] DESTITO et al., 2007: 81. GAROFOLI, 2013: 639.

[78] DESTITO et al., 2007: 81.

[79] DESTITO et al., 2007: 81. DE SANZO et al., 2009: 896.

[80] PECORELLA, 2006: 312.

[81] BORRUSO, 1994b: 28.

[82] DESTITO et al., 2007: 82.

b) CRÍTICA A ESTA OPINIÓN

La doctrina hoy mayoritaria critica fuertemente esta teoría sobre la base, particularmente, de que el sistema informático no puede ser asimilado a los lugares privados expresamente mencionados en el artículo 614 del Código penal italiano (habitación, lugares de privada morada y sus pertenencias), en cuanto lugares de protección espacial de la persona[83]. Las razones que fundamentan tal opinión son dos:

> **a) Mayor amplitud del objeto protegido:** se aduce que la defensa de esta postura plantea serios problemas en relación con la utilización del sistema informático en el ámbito industrial y comercial, así como en el sector público, donde es difícil concebir un derecho al domicilio[84].
>
> **b) Contradicción con el elemento medidas de seguridad:** también se afirma que el verdadero condicionante de la tipicidad de la conducta es la vulneración de medidas de seguridad y no el consentimiento, esto es, la mera voluntad del titular expresada en el derecho de exclusión[85].
>
> **c) Inviabilidad de la aplicación del concepto tradicional domicilio:** en tanto éste constituye el lugar físico y no ideal de la proyección espacial de la personalidad del sujeto como proyección de la intimidad personal[86]

---

[83] PECORELLA, 2006: 316.

[84] CANNATA, 2006: 524.

[85] CANNATA, 2006: 524. PECORELLA, 2011: 5980.

[86] MARANI, 2007: 311.

2. *RISERVATEZZA INDIVIDUALE* (INTIMIDAD)

Otro sector doctrinal considera que el bien jurídico protegido es la *riservatezza*, un derecho fundamental del individuo consagrado en el artículo 2 de la Constitución italiana[87]. Mientras algunos autores hacen referencia, concretamente, a la *riservatezza* de las comunicaciones y de la información[88] otros, en cambio, la vinculan a los datos y programas contenidos en el sistema informático[89].

Por lo que respecta a su contenido, la *riservatezza* se concibe como el interés exclusivo del titular en cuanto a disponer, gozar y controlar los datos, informaciones y procedimientos del sistema y del espacio informático[90]. Según los defensores de esta corriente, esta concepción, que supone entender el tipo como un delito de peligro abstracto, se adapta mejor a la *ratio* teleológica de la norma y a la realidad criminológica del fenómeno del acceso abusivo[91].

---

[87] CECCACCI, 1994: 70. VICARIOLI, 2008: 245.

[88] DELPINO, 2003: 584.

[89] Entienden CORRIAS LUCENTE y POMANTE que debe tenerse en cuenta la calidad de los datos a proteger, siendo que, en su opinión, los únicos datos a los que puede dar amparo este delito son los que tengan un carácter personalísimo, es decir, aquellos que tengan un carácter íntimo o personal. CERQUA, 2000: 53. CORRIAS LUCENTE, 2001: 499. MANTOVANI, 2011: 545. MERLI, 1993: 127. NUNZIATA, 1996: 44. PAZIENZA, 1995: 80. PECORELLA, 2011: 5980. PECORELLA, 2006: 335. POMANTE, 1999: 25-26. TRENTACAPILLI, 2002: 1283-1286.

[90] PECORELLA, 2011: 5980.

[91] Afirma MANTOVANI que esta configuración del bien jurídico permite atender tanto a una función incriminatoria primaria, concretada en la punición de la indiscreción informática, cuanto a una función incriminatoria secundaria, dirigida al uso no autorizado del sistema informático ajeno. Explica PECORELLA que se trata de una solución coherente con la experiencia criminológica de la cual emerge que el acceso abusivo a un sistema informático tiene como objetivo constantemente la adquisición indebida del material contenido en el sistema. MANTOVANI, 2011: 522. PECORELLA, 2006: 316. PECORELLA, 2011: 5980.

3. OTROS BIENES JURÍDICOS

Finalmente, entre la doctrina italiana también se alzan voces que reconocen como objeto tutelado otros bienes jurídicos tales como el delito al **patrimonio**[92], la **utilización del bien informatico**[93], o, ya sea de forma conjunta con la riservatezza o de forma independiente, a la **integridad del sistema y/o de los datos**, de los programas y de la información contenida en el sistema informático[94]. También se hace referencia a las propias comunicaciones e informaciones[95] o a un compendio de los anteriores[96].

Recientemente, la literatura italiana se está decantando por defender una tesis, en mi opinión, próxima a la *riservatezza* pero más centrada en el fenómeno informático. Así se afirma que el bien jurídico protegido es la **intimidad informática**, entendida ésta como un espacio virtual de control y libre disponibilidad del individuo sobre el sistema[97].

---

92 Así lo indica AMORE et al., 2006: 96.

93 BERGHELLA y BLAIOTTA, 1995: 2330.

94 Estos autores afirman que se tutelan las distintas conductas que podrían resultar directamente o indirectamente peligrosas para los elementos de los que se integra el sistema. La base jurídica de esta opinión se halla en la circunstancia agravante prevista en el párrafo 2º del apartado 3 del artículo 615 *ter*, que incrementa la pena por razón del carácter público o militar del sistema informático agredido. Y en general, desde esta perspectiva se concibe el tipo como un delito de peligro abstracto que no requiere la destrucción, producción de un daño o interrupción del funcionamiento del sistema informático o de los datos o programas contenidos en él. CANNATA, 2006: 526. PECORELLA, 2006: 321. MANTOVANI, 1994: 19. MARANI, 2007: 385. MERLI, 1993: 126. NUNZIATA, 1998: 715. También lo defendió en su día PICOTTI, 2004b: 76. MANTOVANI, 1994: 12. MERLI, 1993: 117.

95 DI PUNZIO y NATALINI, 2006: 698.

96 CUOMO y IZZI, 2002: 1018, 1021.

97 Afirman estos autores que el bien jurídico protegido es la mayor utilidad que el usuario consigue a través de la utilización y goce exclusivo del espacio virtual en el que consiste el sistema y que permite un libre desarrollo y una libre exteriorización de la persona humana. PICOTTI, 2000: 20. SALVADORI, 2012: 119-120.

D) TIPO OBJETIVO

1. CONDUCTA

El artículo 615 *ter* del Código penal italiano recoge un tipo mixto alternativo[98] que puede culminarse bien a través de la acción de introducirse en un sistema informático vulnerando las medidas de seguridad dispuestas para impedirlo, o bien a través de la de mantenerse en él sin el consentimiento del titular.

a) ACCESO ABUSIVO

Son numerosas las definiciones que ha ofrecido la doctrina italiana del concepto de acceso aunque, en general todas ellas pueden aunarse en dos grupos sobre la base de si se exige[99] o no[100] la toma de conocimiento sobre el contenido del sistema. En cualquier caso, existe un engranaje común a todas las definiciones propuestas y es que unánimemente se concibe la acción de acceder como **cualquier forma de intromisión sin ulteriores consecuencias en un sistema informático ajeno**[101].

Los puntos más importantes relativos a los elementos del tipo objetivo a comentar en relación con el acceso ilícito son los siguientes:

---

[98] A pesar de entender que se trata de un tipo mixto alternativo, la doctrina italiana afirma que existe una relación de subsidiariedad entre ambas conductas, de forma que la conducta de acceso abusivo es principal o introductoria de la de mantenimiento, cuya comisión típica únicamente podrá tener lugar tras un previo acceso lícito no delictivo y sin vulneración de las medidas de seguridad dispuestas para impedir el acceso. DESTITO et al., 2007: 87. PECORELLA, 2006: 349. PICA, 1999: 42.

[99] ATERNO, 2000: 2990. CECCACCI, 1994: 71. MAIORANO, 2010: 1357. MANTOVANI, 2011: 543. TRENTACAPILLI, 2002: 1283.

[100] BORRUSO, 1994b: 32. CUOMO y RAZZANTE, 2009: 96. GALDIERI, 1996: 48. MARANI, 2007: 618. PICA, 1999: 41. VICARIOLI, 2008: 246.

[101] MARANI, 2007: 618.

i) CONSUMACIÓN Y TENTATIVA

El principal tema de disputa se centra, por tanto, en la **consumación** del delito. Así pues, mientras muy minoritariamente se afirma que ésta se produce con la consecución de un mero contacto con el sistema informático[102], la doctrina mayoritaria entiende que no tiene lugar hasta que se han superado las medidas de seguridad dispuestas para impedir el acceso y, con ello, se ha obtenido disponibilidad sobre el sistema[103]. Una tercera postura va un poco más allá y exige la efectiva toma de conocimiento sobre el contenido del sistema informático[104].

Mientras que las dos primeras opciones conducen a la doctrina italiana a optar, habitualmente, por la configuración del delito como un **tipo de peligro abstracto** y de **mera actividad**, la última de las posturas enunciadas suponen unánimemente configurarlo como un tipo de lesión[105].

---

[102] MARANI, 2007: 618. FONDAROLI, 1996: 312.

[103] ANTOLISEI, 2008: 240. ALIBRANDI, 2011: 1756. BORRUSO, 1994a: 28. CANNATA, 2006: 538. CARINGELLA et al., 2010: 1054.. CECCACCI, 1994: 71. CUOMO y RAZZANTE, 2009: 96. DE SANZO et al., 2009: 898. DELPINO, 2003: 585. DESTITO et al., 2007: 89. GAROFOLI, 2013: 644, 648. GATTA, 2011a: 300. MAIORANO, 2010: 1357, 1368. MELONI, 2012: 2994. PARODI y CALICE, 2001: 64, 66. PECORELLA, 2006: 335-336. PECORELLA, 2011: 5982, 5985, 5987. PICA, 1999: 57.

[104] CADOPPI et al., 2011: 535-536. CANNATA, 2006: 537. MANTOVANI, 2011: 543, 544, 546. NUNZIATA, 1998: 715. RELLA, 2007: 43. VITARELLI, 2011: 399.

[105] Suele tratarse como un delito instantáneo y de efectos prolongados que se perfecciona en el exacto momento en el que se ha superado la última barrera de protección y cuyos efectos se alargarían hasta el momento en el que el sujeto abandonara el sistema informático. PICA, en cambio, entiende que se trata de un **delito permanente**. (Pica, 1999: 57-58) **Delito instantáneo:** CARINGELLA et al., 2011: 1054. DESTITO et al., 2007: 89. GAROFOLI, 2013: 648. MAIORANO, 2010: 1357. MUCCIARELLI, 1996: 101. PECORELLA, 2011: 5987. RELLA, 2007: 43. VICARIOLI, 2008: 247. Entienden que se trata de un delito de **consumación anticipada:** PARODI y CALICE, 2001: 67. Delito de efectos prolongados: VICARIOLI, 2008: 240. CARINGELLA et al., 2010: 1054. DESTITO et al., 2007: 89. PECORELLA, 2011: 5987.

La admisión de la **tentativa**, en cambio, resulta una cuestión bastante menos discutida entre los distintos partidarios de una y otra corriente. Así pues, muchos autores se decantan por admitirla aun entendiendo que el tipo constituye un delito de peligro abstracto, mientras otros consideran que ello constituiría un adelantamiento excesivo de la barrera punitiva, por lo que se manifiestan contrarios a su admisibilidad[106].

ii) TIPOS DE ACCESO

La doctrina italiana hace referencia, en tanto modalidades de comisión del delito de acceso abusivo, a **dos tipos de acceso**: físico o directo y lógico o remoto. No obstante, no toda la doctrina admite ambos tipos de acceso[107]. Un sector considera que la última forma de acceso mencionada, la remota, es el único procedimiento posible de comisión de este delito y niega, por tanto, que el acceso físico pueda considerarse típico[108] reconduciendo su punición a otras normas del Código penal como, por ejemplo, el allanamiento de morada[109].

---

[106] **a) No admiten la tentativa**: CANNATA, 2006: 538. DOLCINI y MARINUCCI, 2011: 5988. ANTOLISEI, 2008: 247. o 222 y MUCCIARELLI, 1996: 101.

b) Sin embargo, admiten la tentativa: ALIBRANDI, 2011: 1756. BORRUSO, 1994b: 28. CARINGELLA et al., 2011: 1054. CECCACCI, 1994: 70-71. DELPINO, 2003: 585. DESTITO et al., 2007: 89. DE SANZO et al., 2009: 898. GAROFOLI, 2013: 646, 648. GATTA, 2011a: 300. MAIORANO, 2010: 1357, 1368. MARANI, 2007: 619, 621. MELONI, 2012: 2994. PARODI y CALICE, 2001: 64. PECORELLA, 2006: 336. PECORELLA, 2011: 5982, 5985, 5987. PICA, 1999: 57. RELLA, 2007: 834.

[107] DESTITO et al., 2007: 84 nota 9. DELPINO, 2003: 585. DOLCINI y MARINUCCI, 2011: 5985. GALDIERI, 2001: 81. DI GIANNANTONIO, 1997: 435. PICA, 1999: 42.

[108] D'AIETTI, 1994a: 68-69. CUOMO y RAZZANTE, 2009: 97. MAIORANO, 2010: 1357. PARODI, 2000: 653. PICA, 1999: 41. FIANDANCA y MUSCO, 2013: 293. TRENTACAPILLI, 2002: 1283. MARANI, 2007: 618. PARODI y CALICE, 2001: 64, 67.

[109] CUOMO y RAZZANTE, 2009: 97. DELPINO, 2003: 585. MAIORANO, 2010: 1357.

iii) VULNERACIÓN DE MEDIDAS DE SEGURIDAD

La aceptación de una u otra forma condicionará la configuración de un elemento fundamental para la tipicidad: la **vulneración de medidas de seguridad**. Como se ha anunciado, el ámbito aplicativo del precepto se ve restringido por una limitación, la exigencia de que el acceso se produzca mediante la superación de los medios de protección dispuestos para impedir dicho acceso.

Aunque la doctrina italiana ha pretendido restar importancia a este elemento, lo cierto es que éste actúa como un criterio de selección de la tutela penal, que se halla limitada únicamente a los sistemas informáticos o telemáticos protegidos por medidas de seguridad, quedando fuera del ámbito típico todos aquellos que no dispongan de tales medidas[110].

En general, la concreción de este elemento se lleva a cabo por la doctrina partiendo desde una doble perspectiva: por una parte, atendiendo al objeto en el que se materializan las medidas

[110] Efectivamente, cierto sector de la doctrina ha intentado vincular la vulneración de las medidas de seguridad al consentimiento, considerando que este elemento no constituye más que la expresión de la voluntad del titular del *ius excludendi*, es decir, la manifestación explícita de la ausencia de conformidad de titular del sistema con la realización de la conducta. DESTITO Y DEZZANI afirman que para poderse hablar de domicilio informático en tanto espacio de pertenencia exclusiva del sujeto con prohibición de la intrusión de otros sujetos sin autorización específica y expresa del titular, en el sentido exigido por el tipo, es necesario que ésta sea patente e inequívoca en cuanto a la exclusión de terceros, hecho al que contribuye la previsión de la vulneración de medidas de seguridad. Entender que la exigencia de vulneración de las medidas de seguridad tiene como fin único la exteriorización del consentimiento implica *a sensu contrario* presumir *iuris tantum* que existe conformidad al acceso en todos aquellos sistemas que no disponen de medidas de seguridad, algo que no es verdad. DESTITO et al., 2007: 83. PICA, 1999: 43. CADOPPI et al., 2011: 533. TRENTACAPILLI, 2002: 1283. MAIORANO, 2010: 1360. PECORELLA, 2011: 5983.

de seguridad[111], y, por otra, atendiendo a la finalidad que estas deben satisfacer, esto es, la exclusión de terceros[112] o la reserva del contenido[113]. Así pues, las medidas de seguridad han sido definidas por la doctrina como el conjunto de dispositivos idóneos para impedir el acceso al sistema a los sujetos no autorizados[114]

Como corolario de lo anterior y en plena ilación con los dos tipos de acceso comentados, puede distinguirse dos tipos de medidas, las físicas o materiales o lógicas o inmateriales. Y, al igual que sucedía respecto de los tipos de acceso, no existe consenso unánime a los efectos de aceptar una u otras[115].

---

111 BORRUSO et al., 1994: 29. CADOPPI et al., 2011: 532. CANNATA, 2006: 534. CECCACCI, 1994: 71. CUOMO y RAZZANTE, 2009: 100. FIANDANCA y MUSCO, 2013: 294. MANTOVANI, 2011: 545. PECORELLA, 2011: 5984. PICA, 1999: 53.

112 AMORE et al., 2006: 100. CARINGELLA et al., 2010: 1052-1053. CRESPI et al., 2011: 2334. CATULLO, 2004: 930. D'AIETTI, 1994b: 72. PECORELLA, 2011: 5983. FIANDANCA y MUSCO, 2013: 294. MUCCIARELLI, 1996: 99. PICOTTI, 2004: 22.

113 BORRUSO et al., 1994: 28. CERQUA, 2000: 53. CUOMO y IZZI, 2002: 1021. MANTOVANI, 2011: 518-521. PECORELLA, 2011: 5983. TRENTACAPILLI, 2002: 1283. Relazione di presentazione dello Schema di Progetto di legge contenente modificazioni ed integrazioni delle norme del Codice penale in tema di criminalità informática, Documenti Giustizia, 1991, n. 9, 142 y ss.

114 MANTOVANI, 2011: 545.

115 Un sector muy minoritario de la doctrina penal italiana (a) excluye de la noción jurídica de medidas de seguridad tanto los medios de carácter físico como algunos de tipo lógico. Otro sector (b), en cambio, entiende que deben quedar englobados tanto los mecanismos de tipo lógico como los de tipo físico, pero dentro de éstos últimos, solo los instalados directamente sobre el sistema. Finalmente, algunos autores (c) incorporan también los elementos dispuestos para proteger la entrada al lugar donde éste se encuentra. **a)** BERGHELLA y BLAIOTTA, 1995: 2334. CECCACCI, 1994: 70. CUOMO y RAZZANTE, 2009: 101. **b)** BORRUSO et al., 1994: 29. CADOPPI et al., 2011: 535. CANNATA, 2006: 535-536. CARINGELLA et al., 2010: 1053. FONDAROLI, 1996: 291. GALDIERI, 1997: 154. LATTANZI y LUPO, 2010: 1360. MANTOVANI, 2011: 521 y 545. PLANTAMURA y MANNA, 2007: 45-46. **c)** ALIBRANDI, 2011: 1758. CRESPI et al., 2011: 2334. DELPINO, 2003: 585. DESTITO et al., 2007: 84. FIANDANCA y MUSCO, 2013: 294. GALDIERI, 1997: 154. PALAZZO y PALIERO, 2011: 300. PICA, 1999: 52. PECORELLA, 2006: 326. sssPICOTTI, 2004a: 22. MARANI, 2007: 617.

A diferencia de lo que sucede con la naturaleza y tipología de medidas de seguridad que deben considerarse admisibles a los efectos de afirmar la tipicidad del acceso abusivo a un sistema informático, la cuestión en la que coincide la doctrina italiana es en cómo se produce la vulneración de las medidas de seguridad, hecho que se hace depender de tres factores: la presencia de éstas, su idoneidad y su superación[116].

a) Presencia: se traduce en la actualidad de la medida, en el sentido de que realmente exista y que se encuentre activa en el momento del acceso[117].

b) Idoneidad: vinculación directa entre la medida y el fin de exclusión pretendido[118].

c) Superación: se produce cuando éstas son efectivamente desactivadas o sobrepasadas como consecuencia de la voluntad quebrantadora y anulatoria de quien accede ilícitamente al sistema[119].

---

[116] Afirma PLANTAMURA que los índices de valoración para entender producida la vulneración deberían atender a la naturaleza y a la finalidad de lo accedido, la idoneidad de la intervención a lesionar o poner en peligro los objetivos a los cuales resultaba instrumental la protección del sistema y los datos en él contenido, esto es, la existencia al menos de prohibiciones o límites a conocer o a utilizar los contenidos del área informática accedida, y en fin, las funciones desarrolladas por el sujeto activo en seno a la organización titular del sistema protegido. PLANTAMURA y MANNA, 2007: 46.

[117] AMORE et al., 2006: 106. CUOMO y RAZZANTE, 2009: 101. CERQUA, 2000: 53. DESTITO et al., 2007: 83. FAVA, 2009: 898. PECORELLA, 2006: 327. PECORELLA, 2011: 5983. PICA, 1999: 44. PLANTAMURA y MANNA, 2007: 46.. FLOR, 111

[118] MAIORANO, 2010: 1360. TRENTACAPILLI, 2002: 1283.

[119] CUOMO y RAZZANTE, 2009: 101.

b) MANTENIMIENTO ABUSIVO

La segunda de las conductas previstas en el artículo 615 ter es la relativa al mantenimiento abusivo en un sistema informático en contra de la voluntad expresa o tácita de quien tenga un legítimo derecho de exclusión. Esta conducta viene a integrar la **modalidad pasiva del allanamiento de domicilio informático,** a imagen y semejanza de su homónimo no informático.

La doctrina italiana inserta dentro del ámbito típico de esta modalidad **cuatro supuestos**: el abuso de la legitimación que se ostenta sobre el sistema informático al ir más allá de los límites modales o temporales establecidos u objeto de concesión[120]; los supuestos de revocación del consentimiento[121]; el acceso involuntario o casual de buena fe con mantenimiento doloso[122]; y el abuso en el acceso cuando se ostenta únicamente una autorización excepcional para la realización de unas operaciones muy concretas[123].

---

[120] La norma castiga o bien la superación de los límites de temporalidad expresos determinados por la voluntad del titular o bien a quien, ostentando un título para acceder al sistema, utiliza a éste para una finalidad diversa a aquella que ha sido consentida. BORRUSO, 1994b: 32. CUOMO y RAZZANTE, 2009: 97. DE SANZO et al., 2009: 898. MONACO, 2011: 2334. PICA, 1999: 41. MAIORANO, 2010: 1357. CUOMO, 2000: 300. PECORELLA, 2006: 349. CANNATA, 2006: 450. GATTA, 2011b: 301. MUCCIARELLI, 1996: 101. PICA, 1999: 41. RELLA, 2007: 43.

[121] Para PICA, en cambio, este comportamiento siempre es activo, nunca omisivo, porque la voluntad de la norma está integrada por la petición de abandono por parte del titular del sistema y la acción de mantenimiento voluntario del sujeto activo del delito. MAIORANO, 2010: 1356. MARANI, 2007: 618. MUCCIARELLI, 1996: 100. VICARIOLI, 2008: 246. PICA, 1999: 41-42.

[122] El sujeto debería, una vez advertida su presencia lícita en el sistema, cerrar la conexión o buscar el camino de salida. BORRUSO, 1994b: 32. CANNATA, 2006: 450. PECORELLA, 2011: 5987. PECORELLA, 2011: 351. FONDAROLI, 1996: 312. MARANI, 2007: 618. VICARIOLI, 2008: 246.

[123] PARODI, 1998: 1040. PECORELLA, 2006: 351.

i) CONSUMACIÓN Y TENTATIVA

Esta acción de mantenimiento integra según opinión unánime de la doctrina un delito de **mera actividad** que se consuma con la mera permanencia[124] en el sistema sin consentimiento del titular o titulares del mismo. Además, se trata de un delito de **carácter permanente**, puesto que sus efectos se prolongan hasta el abandono del sistema por parte el sujeto activo[125].

ii) CONSENTIMIENTO

El elemento de mayor relevancia para entender producida la tipicidad objetiva viene integrado por el consentimiento, que viene manifestado en la expresión *en contra de la voluntad expresa o tácita del titular del derecho de exclusión* y que determina, como se ha visto en el párrafo anterior, el **momento consumativo de la conducta**.

En este sentido, es suficiente con que pueda eliminarse toda duda de que existió una voluntad tácita del titular dirigida a la exclusión del sujeto activo de la permanencia en el sistema[126]. Ello se traduce, por tanto, en una **constancia expresa**, que no manifestación expresa, de la ausencia de consentimiento por parte del titular de algún derecho sobre el sistema[127].

---

[124] La perfección típica se produce de igual forma que en el delito de allanamiento de morada con la mera acción de permanecer en la morada sin que sea necesario ningún efecto o resultado adicional. CANNATA, 2006: 451. PARODI, 1998: 1040.

[125] En contra, DESTITO, DEZZANI y SANTORIELLO consideran que se trata de un delito instantáneo de efectos prolongados para ambas modalidades, que se perfecciona en el momento y lugar del acceso o la permanencia y cuyos efectos se prolongan hasta que el sujeto abandona el sistema informático. CARINGELLA et al., 2011: 1054. DESTITO et al., 2007: 89. GAROFOLI, 2013: 648. RELLA, 2007: 43.

[126] CUOMO, 2000: 2990. CUOMO y RAZZANTE, 2009: 97. DELPINO, 2003: 585. LUSITANO, 1998: 1923. MARANI, 2007: 618, 621. PECORELLA, 2006: 351-352.

[127] CANNATA, 2006: 538. VICARIOLI, 2008: 247.

c) OBJETO MATERIAL: SISTEMA INFORMÁTICO/ TELEMÁTICO

El artículo 615 *ter* adopta como objeto material del delito no solo el sistema informático, sino también el sistema telemático. A pesar de que en ocasiones la doctrina considera que se trata de conceptos sinónimos, en realidad establece una clara diferencia entre uno y otro sistema, que radica en la **función que cada uno de ellos cumple**. Así pues, mientras el primero estaría destinado al tratamiento de datos informáticos, el segundo tendría como misión la recepción y transmisión de los mismos[128].

El Código penal italiano no ofrece una definición de sistema informático, habiendo sido la doctrina y la jurisprudencia los encargados de perfilarlo. A tal efecto, la definición que más se repite es la recogida en la *Cassazione penale, Sezione VI, 14 dicembre 1999, nº 3067*, que le atribuye una composición integrada por **tres elementos funcionales**: el registro o almacenamiento de datos, el procesamiento automático de los datos registrados o almacenados, y la organización de estos datos[129].

---

[128] CANNATA, 2006: 531-532. CUOMO y RAZZANTE, 2009: 94-95. MARANI, 2007: 615.

[129] *Cass. pen., Sez. VI, 14 dicembre 1999, n. 3067. Deve ritenersi «sistema informatico», secondo la ricorrente espressione utilizzata nella legge 23/12/1993, n. 547 che ha introdotto nel codice penale i cosiddetti computer's crimes, un complesso di apparecchiature destinate a compiere una qualsiasi funzione utile all'uomo, attraverso l'utilizzazione (anche parziale) di tecnologie informatiche, che sono caratterizzate - per mezzo di un'attività di «codificazione» e «decodificazione» - dalla «registrazione » o «memorizzazione», per mezzo di impulsi elettronici, su supporti adeguati, di «dati», cioè di rappresentazioni elementari di un fatto, effettuata attraverso simboli (bit), in combinazione diverse, e dalla elaborazione automatica di tali dati, in modo da generare «informazioni», costituite da un insieme più o meno vasto di dati organizzati secondo una logica che consenta loro di esprimere un particolare significato per l'utente. La valutazione circa il funzionamento di apparecchiature a mezzo di tali tecnologie costituisce giudizio di fatto insindacabile in Cassazione ove sorretto da motivazione adeguata e immune da errori logici.*

d) LA EXPRESIÓN *ABUSIVAMENTE*

El tenor literal del precepto exige que las dos conductas estudiadas se realicen de forma abusiva, elemento que tanto la doctrina como la jurisprudencia han considerado expresión nuclear de la **antijuricidad de la conducta** y han equiparado a la ausencia de consentimiento por parte del titular, esto es, el *ius excludendi*[130]. Esta postura es totalmente unánime, al considerarse que el elemento de la abusividad así entendido se integra plenamente en una estructura típica que, como cabe recordar, se ha construido en el ámbito italiano a semejanza del allanamiento de morada[131].

Además, de acuerdo con la jurisprudencia italiana, la valoración de este elemento debe realizarse en un **sentido objetivo**, con referencia a la hora de acceso y a cómo el autor neutraliza y supera las medidas de seguridad que ha dispuesto el propietario del *ius excludendi*, ello con el fin de impedir el acceso indiscriminado al sistema[132].

---

[130] La doctrina se plantea, al efecto, si las expresiones abusivamente y en contra de la voluntad de quien tenga el legítimo derecho de exclusión pueden considerarse dos requisitos expresivos de la antijuricidad con el mismo contenido o, por el contrario, debe atribuírseles contenido diverso. Algunos autores (VICARIOLI) consideran que este elemento no conforma expresión de la tipicidad sino de la antijuridicidad general, al entender que el consentimiento es una causa de justificación y no de ausencia de tipicidad. Otros entienden que el adverbio abusivamente introduce una nota de antijuricidad especial que hace que la conducta típica sea difícil de delimitar y que retrasa la declaración de impunidad de un hecho al ámbito de las causas de justificación. CANNATA, 2006: 541-542. MANTOVANI, 2011: 520. PAZIENZA, 1995: 756. PECORELLA, 2011: 5986. PICA, 1999: 51. Véase también FONDAROLI, 1996: 312. MUCCIARELLI, 1996: 100. VICARIOLI, 2008: 246.

[131] CANNATA, 2006: 541.

[132] *Cass. pen., Sez. V, 25 giugno 2009, n. 40078. Ai fini della configurabilità del reato di accesso abusivo a un sistema informatico, la qualificazione di abusività va intesa in senso oggettivo, con riferimento al momento dell'accesso e alle modalità utilizzate dall'autore per neutralizzare e superare le misure di sicurezza apprestate dal titolare dello "ius excludendi", al fine di impedire accessi indiscriminati.*

E) TIPO SUBJETIVO

Desde un punto de vista subjetivo, la doctrina requiere únicamente un **dolo genérico**, consistente en la voluntad de introducirse o de mantenerse en la memoria interna del sistema informático, en ausencia del consentimiento del *ius excludendi*, y con el conocimiento de que éste ha dispuesto medidas de seguridad para impedir el acceso a los datos que se encuentran en él[133]. En este sentido, la finalidad subjetiva perseguida por el autor en la realización de la conducta es de todo punto irrelevante, de modo que no se exige la concurrencia de **ningún elemento subjetivo del injusto**[134].

F) PENA

El artículo 615 *ter* prevé un tipo básico y, como se ha indicado anteriormente, un subtipo agravado. El artículo 615 *quáter* castiga expresamente los **actos preparatorios** del acceso ilícito[135].

---

[133] CANNATA, 2006: 547. CARINGELLA et al., 2011: 1054. CUOMO y RAZZANTE, 2009: 97. DELPINO, 2003: 585. DESTITO et al., 2007: 89. FIANDANCA y MUSCO, 2013: 299. GAROFOLI, 2013: 648. MAIORANO, 2010: 1360. MANTOVANI, 2011: 546. MARANI, 2007: 620. GATTA, 2011a: 301. PARODI y CALICE, 2001: 68. PECORELLA, 2011: 5987. PICA, 1999: 69. RELLA, 2007: 44. VICARIOLI, 2008: 247.

[134] PECORELLA, 2011: 5987.

[135] Art. 615-quater. Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici.

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 617- quater.

IV. ESTADOS UNIDOS DE AMÉRICA

Estados Unidos de América ha sido, sin duda, el país pionero en materia de criminalidad informática, sobre todo por lo que se refiere a acceso ilícito, ello principalmente porque fue el primer país en el que se planteó la necesidad de adoptar legislación penal en la materia[136]. El estudio de la incriminación del acceso ilícito a un sistema informático se presentará en atención a su propia estructura organizativa de carácter político, la federación: en primer lugar se tendrá en cuenta la regulación federal y, posteriormente, se analizarán algunos de los países federados.

A) LEGISLACIÓN FEDERAL

1. MARCO LEGAL

La primera norma federal dirigida a proteger a los sistemas informáticos que contenían datos relevantes para la seguridad nacional fue la *Counterfeit Access Device and Computer Fraud and Abuse Act*, más conocida como la *Computer Fraud and Abuse Act*, adoptada el 12 de octubre de 1984 y que introdujo la Sección 1030 del Título 18 en el Código Federal de Estados Unidos[137].

---

[136] En febrero de 1977, el Senador Abe Ribicoff, Presidente del Comité de Operaciones Gubernamentales del Senado de los Estados Unidos de América, tras un minucioso estudio en cuyas conclusiones se subrayaba la insuficiencia de la legislación estadounidense vigente para afrontar y perseguir conductas reprochables relacionadas con la delincuencia informática, presentó la primera propuesta legislativa nacional para castigar penalmente a nivel federal el uso no autorizado de un ordenador. Aunque el proyecto de ley no fue aprobado, contribuyó a poner de manifiesto al resto del mundo el gran alcance y el potencial efecto dañino de esta nueva forma tecnológica que integran los equipos informáticos. SCHJOLBERG, 2008: 3.

[137] *Title 18, Part I, Chapter 47 § 1030. Fraud and related activity in connection with computers*

La *Computer Fraud and Abuse Act* centró su atención en el acceso no autorizado a un ordenador, estableciendo tres modalidades diferentes de acceso: el acceso no autorizado a un ordenador que contenga información clasificada de defensa nacional o relaciones con el exterior, el acceso no autorizado a un ordenador que contenga cierta información financiera de instituciones financieras, y el acceso no autorizado a un ordenador del gobierno.

Dicha norma recibió importantes críticas a causa de la extrema ambigüedad y parquedad con que definía las conductas, así como porque no tenía en cuenta el ánimo subjetivo del autor, que podía ser criminal pero también simplemente lúdico[138]. Con el fin de completarla, dos años después se aprobó la *Computer Fraud and Abuse Act* (CFAA) que modificó sustancialmente la Sección 1030[139].

---

[138] Por consiguiente, se incriminaban conductas de acceso a un ordenador pero vinculadas al particular carácter de los datos contenidos en los ordenadores, todos ellos relevantes para la seguridad nacional. MENELLY, 1985: online.

[139] La *Computer Fraud and Abuse Act* añadió las expresiones a sabiendas (*knowingly*) o con la intención de (*intentionally*) con el fin de castigar únicamente las conductas dolosas y con las finalidades específicas que en ellas se describen: la obtención de información o una intención específica de defraudar. Se trata de una distinción fundamental porque deja fuera todas aquellas conductas que puedan implicar el acceso a un ordenador sin intención alguna, como el hacking blanco y todos aquellos accesos que tengan un móvil puramente lúdico o de diversión. Al mismo tiempo, añadió una modalidad alternativa de conducta, la de quien habiendo accedido de forma lícita y autorizada usa un ordenador para propósitos que van más allá de lo autorizado u ocasiona una interferencia o un daño en un ordenador utilizado en el comercio o las comunicaciones interestatales. Atribuyó a este nuevo comportamiento el nombre de exceso de autorización (*exceeds authorized access*) y lo definió como el acceso a un ordenador mediante autorización pero con la finalidad de obtener o cambiar información distinta de aquella para la que ésta se ha obtenido (e) (6) the term *exceeds authorized access* means to *access a computer with authorization and to use such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter*.

Con el fin de contribuir también a la lucha contra la delincuencia informática, también ese mismo año fue adoptada por el Congreso de los Estados Unidos la *Electronic Communications Privacy Act*, denominación que engloba la *Electronic Communications Privacy Act*, que regula el *Title 18, Part I, Chapter 119, § 2511 Interception and disclosure of wire, oral, or electronic communications prohibited"* y la *Stored Wire and Electronic Communications and Transactional Records Act*, que introduce el *Title 18, Part I, Chapter 121, § 2701 Unlawful access to stored communications*, las cuales coinciden sustancialmente en diversos aspectos[140].

Aunque fueron sucesivas las enmiendas a tales textos, la tres reformas más reseñables a dichas normas se produjeron en 1996, 2001 y en 2008 a través de la *National Information Infrastructure Protection Act*, la *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act* de 2001, más conocida como USA Patriot Act, hoy en gran parte derogada y la *Ciber-Crime Act* de 2007[141], respectivamente.

---

[140] El origen de ambas normas se halla en la *Omnibus Crime Control and Safe Streets Act* de 1968, más conocida como la *Federal Wiretap Act* o el *Wiretap Statute*, la cual iba dirigida a prohibir la interceptación ilícita y no consentida de las conversaciones telefónicas. Mientras que la *Computer Fraud and Abuse Act* incriminaba el acceso a ordenadores que contuvieran información reservada de seguridad nacional o entidades financieras, la *Electronic Communications Privacy Act* y la *Stored Wire Electronic Communications and Transactional Records Act* iban dirigidas a prohibir el acceso no autorizado a comunicaciones por cable o electrónicas y a los contenidos que en ellas se transmiten. Sin embargo, las definiciones que recogen resultan compatibles con las que ofrecía la *Computer Fraud and Abuse Act*.

[141] Esta modificación tuvo lugar para adaptar la legislación nacional al Convenio sobre Cibercrimen. Estados Unidos de América ratificó el Convenio de Cibercrimen el 29 de septiembre de 2006 con una reserva por lo que concernía al acceso ilícito: *En aplicación de los artículos 2 y 40 del Convenio, Estados Unidos de América declara que, en virtud de la legislación de Estados Unidos, el delito tipificado en el artículo 2 («Acceso ilegal») incluye como requisito complementario la intención de obtener datos informáticos.*

2. LITERALIDAD DE LA NORMA

En la Sección 1030 se castigan dos conductas:

Según se haya obtenido información:

a) 1030 (a) (1) información del Gobierno de los Estados Unidos clasificada por Decreto presidencial o que requiera protección ante el acceso no autorizado por motivos de defensa nacional o de relaciones exteriores, o cualquier otro dato restringido.

b) 1030 (a) (2) contiene tres supuestos:

(A) información contenida en un registro financiero de una institución financiera o de un emisor de la tarjeta o contenida en un archivo de una agencia de información sobre el consumidor

(B) información de cualquier departamento o agencia de los Estados Unidos

(C) información de cualquier ordenador protegido

Si no se ha obtenido información, se castiga el mero acceso o el exceso de autorización al ordenador en los siguientes casos:

a) 1030 (a) (3) Cuando se trate de un ordenador no público de un departamento o agencia de los Estados Unidos.

b) 1030 (a) (5)

(A) Cuando se cause un daño sin autorización a una computadora protegida a través de la transmisión de un programa, información, código o comando.

(B) Cuando éste daño se cause de forma imprudente.

(C) Cuando se cause pérdida y daño.

3. ELEMENTOS DEL TIPO OBJETIVO

a) MODALIDADES TÍPICAS

La Sección 1030 del Código Penal Federal de Estados Unidos aparece conformada por diversos delitos con una configuración nada uniforme. En conjunto se prevén dos modalidades típicas: el acceso sin autorización y el acceso excediendo la autorización, que no se castigan en relación con todas las conductas. Además, el objeto material del delito, que generalmente es el ordenador y no el sistema informático, se restringe en mayor o menor medida en atención a la gravedad o intensidad del injusto.

El mero acceso a un ordenador aparece recogido en la Sección 1030(a)(3)[142] (de escasa aplicación práctica[143]), pero solo se castiga cuando se produce sin autorización y no en exceso en la autorización[144] y cuando afecta a ordenadores no públicos de los Estados Unidos de América que tienen un uso exclusivo por y para el país, es decir, tanto si son usados exclusivamente por el Gobierno o éste comparte su acceso con otros[145].

---

[142] *(3) intentionally, without authorization to access any nonpublic computer of a department or agency of the United States, accesses such a computer of that department or agency that is exclusively for the use of the Government of the United States or, in the case of a computer not exclusively for such use, is used by or for the Government of the United States and such conduct affects that use by or for the Government of the United States.*

[143] KERR, 2013: 30.

[144] Además, aunque el comportamiento delictivo que configura el acceso ilícito aparece regulado en la Section 1030, la definición de intruso informático viene recogido en la 2510, entendiendo éste como aquella persona que tiene acceso a un ordenador protegido sin autorización y sin dejar ninguna expectativa razonable de intimidad en cualquier comunicación transmitida a, por, o del ordenador protegido; lo que no incluye a una persona conocida por el propietario o el operador del ordenador protegido con quien éste tenga una relación contractual que le permita acceder a todo o a parte del ordenador protegido.

[145] DOYLE y BARLETT WEIR, 2006: 3.

No obstante, puesto que a lo largo del articulado de dicha Sección son términos utilizados los de acceso, exceso en la autorización y ordenador protegido, éstos serán los que se comenten en el presente apartado.

i) ACCESO

El término acceso es definido como la introducción ilegal de carácter electrónico[146] en el sistema sin ninguna consecuencia ulterior[147]. En Estados Unidos de América este concepto se vincula a las conductas llevadas a cabo por ***outsiders***, es decir, por personas que no tienen ninguna potestad de uso sobre el sistema informático[148].

El acceso sin autorización se encuentra limitado a aquellos casos en los que a el sujeto activo está completamente fuera del Gobierno, y no tiene autoridad para acceder a un ordenador de cualquier agencia o departamento de los Estados Unidos, o cuando el acceso es de carácter interdepartamental, es decir, el sujeto accedente forma parte de un departamento distinto al que pertenece el ordenador el que ha accedido[149].

---

[146] Con base a estas características, la doctrina ha puesto de relieve la extrema peligrosidad de la indeterminación de los márgenes de esta conducta y la necesidad que la esfera de aplicación de la misma esté plenamente fijada. Afirma, en este sentido, que el hecho de que el escaso contenido de injusto y la ausencia de una delimitación clara de la conducta permite a la policía detener a quien ellos consideren oportuno sin someterse al principio de legalidad. KERR, 2013: 31-32. KERR, 2010: 1577.

[147] DOYLE, 2014: 2.

[148] DOYLE y BARLETT WEIR, 2006: 4. MARSHALL y BAILI, 2011: 23.

[149] En este sentido, se han distinguido los casos en los que ha los actos de acceso no autorizado que se producen dentro de un departamento y las que implican delitos en los ordenadores que pertenecen a otro departamento. En el primer supuesto, si se produce un acceso no autorizado a un ordenador del mismo departamento pero sobre el cual no se tiene autorización para acceder, éste deberá quedar relegado a la mera sanción administrativa, no considerándose justificada, necesaria y proporcional la intervención del Derecho penal. DOYLE y BARLETT WEIR, 2006: 4.

ii) EXCESO DE AUTORIZACIÓN

Respecto a la conducta de exceso en la autorización, el sujeto activo ostenta un título jurídico que le permite acceder a la totalidad o a parte del sistema pero con unas facultades concretas. En lugar de criminalizar este supuesto con base a la formulación de una nueva modalidad típica, la Sección 1030 del Código Penal Federal de los Estados Unidos de América hace descansar estructuralmente la tipicidad de la acción en el **consentimiento**[150]. Así, la acción siempre es la misma: el acceso, pero la responsabilidad penal se activa tanto cuando el sujeto accede al sistema en ausencia de consentimiento, esto es, sin autorización (*without authorization*), como cuando, gozando del mismo, existe un exceso en la autorización concedida (*exceeding authorized access*)[151].

La literatura norteamericana vincula directamente la acción con el término de ***insiders*** (por contraposición al acceso sin autorización que sería cometido por *outsiders*), es decir, aquellos sujetos que ostentan algún género de facultad de acceso sobre el sistema informático y la información[152].

---

[150] KARAGIANNOPOULOS, 2014: 466.

[151] Como se ha indicado anteriormente, esta segunda modalidad de comisión de la acción de acceso ilícito fue introducida en la legislación federal de los Estados Unidos de América a través de la *Computer Fraud and Abuse Act de 1986*, pues la Comprehensive Crimen Control Act de 1984 que la precedía como primera respuesta del país en contra del fenómeno denominado en el país como *hacking* informático nada contenía al respecto. La expresión *exceeding authorized access* reemplaza la originaria redacción que era descrita en la Ley de 1984, la cual era descrita como: *having accessed a computer with authorization, uses the opportunity such access provides for pursposes to which authorization does not extend*.

[152] KARAGIANNOPOULOS, 2014: 466. MARSHALL y BAILI, 2011: 5.

Además, el término aparece definido en el apartado (e) (6) de la Sección 1030 de la *Computer Fraud and Abuse Act* como la acción de acceder a un ordenador con autorización y usar dicho acceso para obtener u alterar información en el ordenador para la que el sujeto accedente no está autorizado a obtener u alterar[153].

Uno de los temas más discutidos en la literatura jurídica del país ha sido el hecho de si es necesario o no llegar a obtener conocimiento sobre información contenida en el sistema. Tras varias oscilaciones, la jurisprudencia ha querido instaurar el foco de atención en la propia infracción informática, **separándola de la información contenida** en aquel[154].

Para establecer la **diferencia entre el acceso no autorizado y el exceso en la autorización** se tiene en cuenta el concreto sistema informático sobre el que se disponía autorización. Así, el acceso a partes distintas de un mismo sistema informático constituirá un exceso en la autorización, pero el acceso a un sistema informático distinto aunque éste forme parte de la misma red de área local, se considerará acceso no autorizado[155]. Sin embargo, esta distinción no convence a la doctrina del país, que ha propuesto la derogación de esta modalidad de la conducta[156].

---

[153] Caso International Airport Centers, LLC vs. Citrin en KARAGIANNOPOULOS, 2014: 476-477.

[154] KARAGIANNOPOULOS, 2014: 467.

[155] Caso United States vs. Morris citado en KARAGIANNOPOULOS, 2014: 468. MARSHALL y BAILI, 2011: 4.

[156] KARAGIANNOPOULOS, 2014: 497 y ss.. MARSHALL y BAILI, 2011: 10.

b) OBJETO MATERIAL: ORDENADOR PROTEGIDO

Aunque como se ha visto en el delito de acceso ilícito el objeto material son los ordenadores federales gubernamentales de carácter no público[157], en el resto de infracciones que se prevén en la Sección 1030 éste se amplia a los ordenadores protegidos (*protected computer*). La Sección 1030 (e) (2) (C) establece qué ordenadores deben entenderse englobados al amparo de este concepto[158]:

> (A) exclusivamente para el empleo de una institución financiera o del Gobierno de los Estados Unidos, o, en el caso de un ordenador no exclusivamente para tal empleo, usado por o para una institución financiera o el Gobierno de los Estados Unidos y la conducta que constituye la ofensa afecta aquel empleo por o para la institución financiera o el Gobierno.
>
> (o B) que es usado en o la **afectación de las comunicaciones del comercio exterior o las relaciones exteriores**, incluyendo un ordenador localizado fuera de los Estados Unidos que son usados en una manera que **afecta al comercio o comunicación interestatal o exterior o entre de los Estados Unidos**.

---

[157] DOYLE y BARLETT WEIR, 2006: 5.

[158] (2*) the term "protected computer" means a computer—*

> *(A) exclusively for the use of a financial institution or the United States Government, or, in the case of a computer not exclusively for such use, used by or for a financial institution or the United States Government and the conduct constituting the offense affects that use by or for the financial institution or the Government; or*
>
> *(B) which is used in or affecting interstate or foreign commerce or communication, including a computer located outside the United States that is used in a manner that affects interstate or foreign commerce or communication of the United States.*

El término ordenador protegido no debe entenderse en el sentido de ordenador dotado de medidas de seguridad[159], sino que en él deben incluirse todos los aparatos utilizados o comercio interestatal o extranjero y los ordenadores utilizados por el gobierno federal y las instituciones financieras que actúan[160].

Con la reforma operada por la *Identity theft Enforcement and Restitution Act* de 2008 y por la USA Patriot Act de 2011 se amplió la noción de equipo protegido a aquellos que resultan afectados al comercio interestatal o extranjero o de comunicaciones. 18 USC § 1.030 (e) (2) (B), pudiendo entenderse englobados en el concepto todos los ordenadores públicos o privados, estén o no conectados a Internet, y estén situados en Estados Unidos o el extranjero[161].

---

[159] MARSHALL y BAILI, 2011: 4.

[160] MARSHALL y BAILI, 2011: 4.

[161] En sus inicios la definición de ordenador protegido englobaba únicamente la letra (A) del apartado mencionado. Sin embargo, la jurisprudencia extendió la protección a cualquier ordenador conectado a Internet; sin que se requiera prueba de que el acusado también utiliza Internet para acceder a la computadora o utilizar el ordenador para acceder a Internet. No obstante, no parecía adecuado excluir la tutela de los ordenadores que no disponían de una conexión a Internet y que no eran utilizados por las instituciones gubernamentales o financieros federales. Ello fue solucionado con la aprobación de la *Identity theft Enforcement and Restitution Act* de 2008, a través de la cual se amplió la noción de equipo protegido a aquellos que resultan afectados al comercio interestatal o extranjero o de comunicaciones. 18 USC § 1.030 (e) (2) (B), y con la USA Patriot Act, que incluyó la segunda referencia a la afectación del comercio interestatal o extranjero o las comunicación de los Estados Unidos con la finalidad de permitir perseguir los casos en que un estadounidense accede equipos situados en el extranjero o en los que en el proceso de transmisión de los datos del acceso hay intervención de Estados Unidos. MARSHALL y BAILI, 2011: 4.

B) LEGISLACIÓN DE LOS ESTADOS FEDERALES

Todos los Estados federales han recogido en sus Códigos Penales el delito de acceso ilícito. Sin embargo, con carácter general puede resaltarse que, aun a pesar de su denominación, el contenido del ilícito penal en ocasiones se asemeja más a la normativa federal, basada en la producción de un daño al ordenador. Por este motivo, a los efectos de exposición del presente estudio, se han seleccionado varios Estados en cuyos Códigos penales fácilmente puede observarse la disyuntiva apuntada.

1. ESTADO DE GEORGIA

La § 16-9-93 OCGA recoge el acceso ilegal a un ordenador (*computer trespass*)[162], conducta que consiste en la utilización de un ordenador o de una red de ordenadores sin autorización y con una de las tres finalidades específicas que se mencionan en el texto: borrar, obstruir o interrumpir y alterar o dañar datos o programas informáticos.

---

[162] *Title 16. Crimes and offenses chapter 9. Forgery and fraudulent practices Article 6. Computer systems protection Part 1. Computer crimes*

§ 16-9-93. Computer crimes defined

(b) Computer Trespass. Any person who uses a computer or computer network with knowledge that such use is without authority and with the intention of:

> *(1) Deleting or in any way removing, either temporarily or permanently, any computer program or data from a computer or computer network;*
>
> *(2) Obstructing, interrupting, or in any way interfering with the use of a computer program or data; or*
>
> *(3) Altering, damaging, or in any way causing the malfunction of a computer, computer network, or computer program, regardless of how long the alteration, damage, or malfunction persists shall be guilty of the crime of computer trespass.*

(e) Computer Password Disclosure. Any person who discloses a number, code, password, or other means of access to a computer or computer network knowing that such disclosure is without authority and which results in damages (including the fair market value of any services used and victim expenditure) to the owner of the computer or computer network in excess of $500.00 shall be guilty of the crime of computer password disclosure.

2. ESTADO DE CALIFORNIA

Su Código penal prevé en la § 502(c) (7)[163] el acceso doloso y sin permiso a un ordenador, un sistema informático o una red de ordenadores.

3. ESTADO DE WASHINGTON

El Código penal de Washington establece dos niveles de gravedad en el acceso[164]. De un lado, en la § 9A.52.110 prevé el acceso ilícito de primer grado, que constituye un delito grave, en el cual deben concurrir alternativamente alguna de las dos siguientes circunstancias: que se realice con la intención de cometer otro delito, o bien que el ordenador o base de datos afectada pertenezca a una Agencia del Gobierno. De otro, en la § 9A.52.120 constituye un tipo residual respecto del anterior que castiga todos aquellos accesos en los que no concurran las circunstancias previstas en la Sección anterior. En último lugar, la § 9A.52.130 enuncia la posibilidad de apreciar un concurso de delitos en aquellos supuestos en los que el acceso al ordenador se realice con el fin de cometer un ilícito posterior.

---

[163] *§ 502. c) (7) Knowingly and without permission accesses or causes to be accessed any computer, computer system, or computer network.*

[164] *RCWs > Title 9A > Chapter 9A.52 > Section*

§ 110 Computer trespass in the first degree.

(1) A person is guilty of computer trespass in the first degree if the person, without authorization, intentionally gains access to a computer system or electronic database of another; and

(a) The access is made with the intent to commit another crime; or

(b) The violation involves a computer or database maintained by a government agency.

(2) Computer trespass in the first degree is a class C felony.

§ 120 Computer trespass in the second degree.

(1) A person is guilty of computer trespass in the second degree if the person, without authorization, intentionally gains access to a computer system or electronic database of another under circumstances not constituting the offense in the first degree.

(2) Computer trespass in the second degree is a gross misdemeanor.

§130 Computer trespass — Commission of other crime.

A person who, in the commission of a computer trespass, commits any other crime may be punished for that other crime as well as for the computer trespass and may be prosecuted for each crime separately.

4. ESTADO DE NUEVA YORK

El Código penal del Estado de Nueva York, tras ofrecer un conjunto de definiciones comunes a todas las secciones, recoge el delito de acceso ilícito (*computer trespass*) en la § 156.10[165]. Éste se define como el uso o acceso a un ordenador con la finalidad de cometer un delito posterior o bien con el propósito de conseguir material informático. Admite la posibilidad, por tanto, de que el acceso ilícito al ordenador sea la puerta para la comisión no solo de un delito contra la intimidad sino de cualquier otro.

5. ESTADO DE TEXAS

El Código penal de Texas prevé idénticas definiciones que los anteriores, pero en la previsión de la conducta efectúa una previsión de acceso genérico, que denomina brecha en la seguridad informática (*breach of computer security*), a la que posteriormente se irán añadiendo exigencias a la conducta del autor, principalmente de carácter subjetivo [166].

---

[165] *§ 156.10 Computer trespass.*

A person is guilty of computer trespass when he or she knowingly uses, causes to be used, or accesses a computer, computer service, or computer network without authorization and:

1. he or she does so with an intent to commit or attempt to commit or further the commission of any felony; or

2. he or she thereby knowingly gains access to computer material.

Computer trespass is a class E felony.

[166] *Sec. 33.02. Breach of computer security.*

(a) A person commits an offense if the person knowingly accesses a computer, computer network, or computer system without the effective consent of the owner.

(b) An offense under Subsection (a) is a Class B misdemeanor, except that the offense is a state jail felony if:

(1) the defendant has been previously convicted two or more times of an offense under this chapter; or

(2) the computer, computer network, or computer system is owned by the government or a critical infrastructure facility.

(b-1) A person commits an offense if with the intent to defraud or harm another or alter, damage, or delete property, the person knowingly accesses a computer, computer network, or computer system without the effective consent of the owner.

6. ESTADO DE WISCONSIN

Por último, el Estado de Wisconsin también distingue el daño informático y el acceso ilícito, estableciendo además en la Sección 943.70 (2)[167] dos modalidades distintas de ataque a los datos o los programas informáticos: por una parte, el acceso a un ordenador o a la documentación contenida en él; y, por otro, el descubrimiento de códigos de acceso o cualquier otra forma de información de acceso.

---

[167] *Sección 943.70 (2) Offenses against computer data and programs.*

(a) Whoever willfully, knowingly and without authorization does any of the following may be penalized as provided in pars. (b) and (c):

3. Accesses computer programs or supporting documentation.

6. Discloses restricted access codes or other restricted access information to unauthorized persons.

SEGUNDA PARTE
EL ACCESO ILÍCITO EN EL ARTÍCULO 197.1 *BIS*

CAPITULO II

EL BIEN JURÍDICO PROTEGIDO

EN EL DELITO DE ACCESO ILÍCITO

I. INTRODUCCIÓN GENERAL

El legislador español ha introducido el delito de acceso ilícito a un sistema informático en el Título X del Código penal, rubricado *Delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio*, y, más concretamente, en su Capítulo I, dedicado al *descubrimiento y revelación de secretos*.

Sirva adelantar ahora, puesto que ello será objeto de análisis en un momento posterior, que la ubicación sistemática indicada no es la más adecuada para dar cobijo a esta conducta. La razón de lo anterior estriba en que la utilización de la intimidad como criterio hermenéutico para la interpretación del tipo implica soslayar algunos de los aspectos más básicos de su núcleo esencial.

Sin perjuicio de lo anterior, buscar acomodo en el Código penal español para el delito de acceso ilícito a un sistema informático no es tarea fácil y, a tal efecto, no resulta extraño que el legislador haya errado en la ubicación sistemática del tipo. Por ello, como en tantos otros delitos, la determinación del bien jurídico protegido en el acceso ilícito ha suscitado una amplia y todavía insoluta controversia.

Con mucho ahínco se ha buscado por parte de la doctrina española y comparada la identificación concreta de un objeto jurídico que ligara adecuadamente con las pretensiones y la necesidad de tutela suscitadas en relación con esta conducta. En este sentido, son numerosas y diversas las propuestas que se han realizado al respecto. La intimidad[1], de hecho, no ha sido finalmente la posición por la que ha optado la mayor parte de la doctrina[2], pues un amplio número de autores defienden la tutela de derechos distintos a ésta, algunos de ellos influenciados por las diferentes configuraciones que de este delito se ha hecho a nivel internacional y comparado.

---

[1] HUERTA TOCILDO y ANDRÉS DOMÍNGUEZ, 2002: 26. MATELLANES RODRÍGUEZ, 2008: 62.. RAGUÉS I VALLÈS et al., 2012: 371..

[2] ANARTE BORRALLO y DOVAL PAÍS, 2012: 12..

En este sentido, se han barajado posiciones que van desde la consideración de la innecesariedad de la protección penal en este ámbito, a la confianza en el funcionamiento de los sistemas informáticos[3], el derecho de acceso y conocimiento de la información[4], el patrimonio[5], la comunicación pacífica a través de redes telemáticas[6], llegándose a afirmar, incluso, que Internet[7] o el propio sistema informático[8] constituyen por sí mismos bienes dignos de protección.

En realidad, todas las propuestas anteriores tienen, a mi juicio, un fundamento similar, centrado en los posibles peligros que las nuevas tecnologías pueden entrañar como consecuencia de los riesgos tanto de carácter individual como colectivo que éstas generan para los usuarios, ahondando así en una de las características que mejor definen el Derecho penal de la sociedad de riesgo, a saber, la tutela del pacífico disfrute de las actividades que rodean los actuales focos de riesgo estabilidad[9].

Así pues, todas las nociones apuntadas vienen a desembocar en la misma idea, pues la desconfianza y el uso pacífico y sin cortapisas de las nuevas tecnologías constituyen, en definitiva, caras opuestas de una misma moneda, a la que la mayoría de autores se han dado en proclamar como seguridad informática[10] —otros, en cambio, seguridad en el tráfico informático[11] o seguridad de la

---

[3] CORCOY BIDASOLO, 2007: 10.. GUTIÉRREZ FRANCÉS, 1996: REVISAR..

[4] ANARTE BORRALLO y DOVAL PAÍS, 2012: 12 y 13..

[5] BÜHLER, 1987: 452. HAFT, 1987: 9. ROVIRA DEL CANTO, 2002: 70 y 196.. SIEBER, 1977: 98.

[6] ROMEO CASABONA, 2006a: 187 a 190..

[7] QUINTERO OLIVARES en un estudio de los delitos contra la propiedad intelectual afirma que QUINTERO OLIVARES, 2001: 375..

[8] MATELLANES RODRÍGUEZ, 2004: 4..

[9] MATELLANES RODRÍGUEZ, 2008: 66.

[10] ROVIRA DEL CANTO, 2002: 199, 200, 204.

[11] GONZÁLEZ RUS, 2007: 15-16. MIRÓ LLINARES, 2010: 145 párrafo 1439.

información[12]—. Éste es, en mi opinión, el bien jurídico protegido en el delito de acceso ilícito, el cual a su vez se presenta como una barrera de protección de otro conjunto de derechos mediatamente protegidos.

A estudiar de forma pormenorizada la polémica presentada y a ofrecerle una solución es a lo que se dedica el presente Capítulo, que presentará y analizará cada una de las propuestas planteadas para, finalmente, realizar una propia.

[12] CARRASCO ANDRINO, 2010b: 346. FERNÁNDEZ TERUELO, 2011: 198-199. MORALES PRATS, 2011b: 821. MORALES PRATS, 2011a: 482.

SECCIÓN 1ª

LA INTIMIDAD COMO BIEN JURÍDICO PROTEGIDO EL HOY DEROGADO ARTÍCULO 197.3

I. INTRODUCCIÓN

La Ley Orgánica 5/2010, de 22 de junio, introdujo el acceso ilícito a un sistema informático mediante la formulación de un tipo de equivalencia en el delito de descubrimiento y revelación de secretos, concretamente en el apartado 3 del artículo 197 del Código penal. Para lograr una adecuada conexión entre la conducta que en tal momento se introducía y los dos apartados que la precedían —los tipos básicos de descubrimiento y revelación de secretos— el legislador español se vio obligado a modificar los términos de la descripción típica propuesta por la normativa supranacional, incluyendo elementos distintos a los previstos en ella.

Como se verá en el correspondiente Capítulo[13], la conducta que finalmente fue objeto de incriminación en el Código penal español tomó como objeto material los datos informáticos (*datos contenidos en todo o en parte de un sistema informático*) de igual forma que los dos tipos básicos recogidos en los artículos 1 y 2 del artículo 197, —con el matiz de que el apartado 1 también hace referencia a elementos materiales como cartas, papeles u otros documentos contenidos en soporte físico—. De este modo, en lugar de incriminarse el acceso ilícito a un sistema informático, en realidad, el recién introducido apartado 3 no hacía más que castigar una nueva modalidad de descubrimiento y revelación de secretos, completando (y complementando) a sus predecesores.

Teniendo en cuenta esta idea, establecer cuál era el bien jurídico protegido en el artículo 197.3 implicaba necesariamente determinar cuál era el bien jurídico protegido en los artículos 197.1 y 197.2. A ello se dedicará la presente sección que, en concordancia con lo anterior, se dividirá en dos partes: la primera, dedicada a delimitar qué concreto derecho se tutela en los dos primeros apartados del artículo 197, y la segunda, a analizar conforme a lo expuesto cuál era el interés jurídico objeto de protección en el apartado 3 conforme a la redacción ofrecida por la Ley Orgánica 5/2010, de 22 de junio.

---

[13] Véase Capítulo V.

II. EL BIEN JURÍDICO PROTEGIDO EN EL DELITO DE DESCUBRIMIENTO Y REVELACIÓN DE SECRETOS

Como se ha indicado, el acceso ilícito fue introducido como un tipo de equivalencia en el seno del delito de descubrimiento y revelación de secretos recogido en el artículo 197. El artículo 197 se encuentra enmarcado en el Capítulo I, rubricado *Del descubrimiento y revelación de secretos* del Título X[14] del Código penal, dedicado a los *Delitos contra la intimidad, la propia imagen y la inviolabilidad del domicilio*. Dicho Título consta, además, de un segundo Capítulo, *Del allanamiento de morada, domicilio de personas jurídicas y establecimientos abiertos al público*, que congrega los delitos relativos a la protección de la inviolabilidad del domicilio. Siendo, pues, en el primer Capítulo donde se contuvo regulado inicialmente el acceso ilícito a un sistema informático, el presente comentario obviará el análisis del Capítulo II y se limitará al estudio del bien jurídico protegido en aquél, esto es, en el delito de descubrimiento y revelación de secretos y, más concretamente, en sus tipos básicos recogidos en el artículo 197.

---

[14] El Título dedicado hoy a los delitos contra la intimidad no existía en el anterior Código penal, sino que resultó en su día una novedosa introducción del Código penal de 1995 con la que se perseguía adecuar la regulación penal a la Ley Orgánica 5/1992, y, al mismo tiempo, aunar diversas conductas que se hallaban dispersas a lo largo del articulado del anterior Código penal de 1973 bajo la rúbrica de un Título dedicado genéricamente a los delitos contra la libertad y la seguridad. Así pues, el vigente Código penal concibió con nombre propio el derecho enunciado en el artículo 18 de la Constitución siendo fiel reflejo del mismo, el cual -excluyendo la referencia al honor que halla tutela propia curiosamente en el siguiente Título del Código penal, el XI rubricado *Delitos contra el honor*- hace referencia no sólo al derecho a la intimidad sino también a la propia imagen y a la inviolabilidad del domicilio. Como indica MORALES PRATS, con ello se ha logrado dotar al tratamiento penal de la intimidad de una unidad y coherencia sistemática de la que carecía el anterior Código penal, que era ajeno a las necesidades derivadas del artículo 18 de la Constitución. La ausencia de coherencia se debía, en realidad, a la falta de aplicación del precepto debido a la propia configuración del mismo sobre objetos documentales no informáticos. La introducción de las vulneraciones derivadas del uso ilícito de la informática ha supuesto para este tipo la adquisición de una posición relevante por lo que se refiere a su vertiente aplicativa. BOIX REIG, 1989: 18-19. CARBONELL MATEU y GONZÁLEZ CUSSAC, 2010: 323-324. MORALES PRATS, 2011a: 448. En relación con el antiguo artículo 497 del antiguo Código penal véase COBO DEL ROSAL, 1971: 684, 685, 678.

Como se ve, la rúbrica del Título X del Código penal hace referencia a la intimidad y a la propia imagen, siendo en principio estos dos derechos los tutelados en el Capítulo I. No obstante, a pesar de esta referencia explícita, la alusión que dicha rúbrica realiza a la propia imagen es meramente nominal porque, en realidad, tal y como está configurada en este el tipo penal, la imagen de la persona tan sólo es un instrumento, soporte o forma de invasión de la intimidad[15]. También resultan, a mi juicio, una referencia tangencial en el tipo penal el derecho al secreto de las comunicaciones y la libertad informática o derecho a la protección de datos personales, dos derechos que, aunque no aparecen reflejados en la rúbrica del Capítulo, la doctrina ha considerado también como intereses tutelados en el delito debido a que de ellos aparecen visos en la propia redacción del artículo 197.

La tutela de todos estos derechos resulta ciertamente nula si se tiene en cuenta ya de inicio que sólo será punible aquella conducta en que, viéndose implicado alguno de ellos, también suponga un claro atentado contra la intimidad. La intimidad se instituye, en consecuencia, como único bien jurídico protegido en el delito sin que, además, se le dispense una protección de carácter absoluto[16], —algo, por cierto, totalmente congruente con las exigencias derivadas del principio de intervención mínima o *ultima ratio* que inspira el Derecho penal[17]—.

---

[15] ROVIRA SUEIRO, 1999: 25.

[16] CARMONA SALGADO, 1996: 272. FERNÁNDEZ TERUELO, 2007: 30. ROMEO CASABONA, 2004b: 30. ROMEO CASABONA, 2003b: 514.

[17] Afirma en este sentido SOLA RECHE que la protección meramente fragmentaria del derecho a la intimidad encuentra justificación en la imposibilidad de abarcar mediante la descripción del tipo penal a todas las facetas que representa el derecho a la intimidad en el acontecer de la vida y de las relaciones humanas. A ello se añade el recordatorio de la doctrina de que únicamente deben ser objeto de protección las manifestaciones del derecho a la intimidad con mayor relevancia para las personas y, además, sólo frente a las agresiones más intolerables contra ellas. Por este motivo, las demás vulneraciones de este derecho deberán ser castigadas mediante sanciones de índole civil. Véase SOLA RECHE, 1991: 193-194. Igualmente, ROMEO CASABONA, 2004b: 30, ROMEO CASABONA, 2003b: 515. ORTS BERENGUER y ROIG TORRES, 2001: 19.

Las ideas expuestas en la página anterior se verán con más claridad si se ponen en relación con los dos tipos básicos del delito, recogidos, respectivamente, en los apartados 1 y 2 del artículo 197.

A) BIEN JURÍDICO EN EL APARTADO 1 DEL ARTÍCULO 197

El apartado 1 del artículo 197 tutela la vertiente negativa del derecho a la intimidad[18], es decir, el derecho a excluir intromisiones de terceros en el ámbito propio de desarrollo personal que toda persona posee. Esta esfera de desarrollo personal se puede ver lesionada a través de tres vías, siempre que además en la conducta del sujeto activo concurra la finalidad de vulnerar la intimidad de otro o de descubrir sus secretos[19]: a) el apoderamiento de sus papeles, cartas, mensajes de correo electrónico o cualesquiera otros documentos o efectos personales, b) la interceptación de las telecomunicaciones, y c) la utilización de artificios técnicos de escucha, transmisión, grabación o reproducción del sonido o de la imagen.

Aunque es cierto que cualquier tipo de injerencia en el derecho a la intimidad puede revestir las dos últimas formas enunciadas —la b) y la c)—, esto es, producirse mediante la captación de la imagen (o el sonido) o mediante la interceptación de las comunicaciones, ello no implica que tales bienes hallen protección a través del artículo 197.1. Así pues, si se atiende a todos los elementos de la descripción típica se llega de forma clara a la conclusión de que, en realidad, en este concreto apartado del precepto no se ofrece tutela a tales derechos. Véase de forma pormenorizada como juegan éstos en el plano jurídico a los efectos de la dispensa de protección penal.

---

[18] TOMÁS - VALIENTE LANUZA, 2010: 794.

[19] Ambas finalidades suponen la concurrencia de un ánimo específico añadido al dolo del autor, tendencias subjetivas que algunos autores consideran deberían ser reconducidas únicamente a una, la segunda (vulnerar la intimidad). GONZÁLEZ GUITIÁN, 1986: 172. MORALES PRATS, 2011a: 456. OLMO FERNÁNDEZ-DELGADO, 2009: 85-86. A ello hay que añadir que no se exige como propósito añadido la intención de revelar la información obtenida. TOMÁS - VALIENTE LANUZA, 2010: 798. ORTS BERENGUER y ROIG TORRES, 2001: 20, 28.

1. INTIMIDAD Y PROPIA IMAGEN

Como se ha avanzado previamente, la rúbrica del Título X del Libro II del Código penal hace referencia no sólo al derecho a la intimidad sino también a la propia imagen. Esta escisión constituye reflejo directo del apartado 1 del artículo 18 de la Constitución, precepto que garantiza mediante su tenor literal ambos derechos.

La alusión del Código penal a la propia imagen ha sido muy criticada por la doctrina, al entender, a mi juicio erróneamente, que este derecho no constituye más que una faceta del derecho a la intimidad frente al control visual clandestino tecnológico[20]. En contraposición a las críticas vertidas sobre el precepto, he de decir que, a pesar de que el tenor literal del artículo 197.1 del Código penal hace referencia a la utilización de artificios técnicos de escucha, transmisión, grabación o reproducción de la imagen, en este caso la imagen es, simplemente, el soporte material de un mensaje con otras connotaciones[21], pues en todo caso el precepto exige que el comportamiento típico se realice con un ánimo muy específico: vulnerar la intimidad de otro.

Quedarán, entonces, excluidas del ámbito típico del precepto todas aquellas invasiones de la propia imagen que no revistan también un ataque contra la intimidad, siendo la captación de la persona en su ámbito íntimo lo que integra la tipicidad haciendo surgir la responsabilidad penal. En consecuencia, es la intimidad y no la imagen el elemento principal de la infracción y, en consecuencia, la presencia de esta última es meramente circunstancial.

---

[20] Se afirma, en este sentido, que había constituido un acierto la eliminación de tal referencia del Proyecto de Código penal de 1994, el cual dedicaba el Título XI a los *Delitos contra la propia imagen* como reminiscencia, a su vez, del Proyecto de Código penal de 1992, objeto de una amplia reprobación en la doctrina, e, incluso, en el informe del Consejo General del Poder Judicial realizado por el profesor VIVES ANTÓN. MORALES PRATS, 2011a: 449. ROMEO CASABONA, 2004b: 31. E, igualmente, ROMEO CASABONA, 2003b: 516.

[21] ROVIRA SUEIRO, 1999: 22.

2. INTIMIDAD Y SECRETO DE LAS COMUNICACIONES

El Título X del Libro II del Código penal no incluye en su rúbrica referencia alguna al derecho al secreto de las comunicaciones, pero cierto sector de la doctrina penal ha defendido, a mi juicio erróneamente, el carácter pluriofensivo del delito de descubrimiento y revelación de secretos entendiendo que, además de la intimidad, el precepto salvaguarda este derecho consagrado en el artículo 18.3 de la Constitución[22].

El motivo principal que se aduce al respecto es que la descripción del tipo castiga específicamente las vulneraciones de la intimidad derivadas de la interceptación de las comunicaciones. Sin embargo, aunque la asociación entre intimidad y secreto de las comunicaciones parece inevitable –éste último integra una de las parcelas de la vida privada de las que se pueden derivar riesgos para la intimidad[23]–, en realidad, afirmar que el secreto de las comunicaciones es también interés protegido en el delito de descubrimiento y revelación de secretos transgrede, en mi opinión, la configuración constitucional de este derecho[24]. El Tribunal Constitucional ha separado claramente ambos derechos, atribuyendo un carácter puramente formal al derecho al secreto de las comunicaciones y diferenciándolo de la intimidad, de contenido

---

[22] Considera, sin embargo, RUIZ MIGUEL que el secreto de las comunicaciones tiene una conexión con el derecho a la intimidad mucho mayor de lo que hubiera podido ser la configuración de una libertad de las comunicaciones, de manera que la Constitución, al recoger sólo el secreto de las comunicaciones, omitiendo la libertad de las mismas en su artículo 18.3, no hace sino subrayar la conexión de ese secreto con la intimidad, considerando, quizás, que la libertad de las comunicaciones ya está amparada en el artículo 17.1 RUIZ MIGUEL, 1995: 89. RUIZ MIGUEL, 1995: 76. BALLESTER CARDELL, 1998: 99.

[23] A favor de delimitar los conceptos de intimidad y secreto. BOIX REIG, 1989: 19.

[24] También opina que supone una quiebra del carácter formal que el Tribunal Constitucional ha atribuido al artículo 18.3 de la Constitución: ELVIRA PERALES, 2007: 22.

marcadamente material[25]. Es posible distinguir, al efecto, dos planos: el del secreto (artículo 18.3), con un carácter formal –garantía formal de intangibilidad[26]– y basado en la presunción *iuris et de iure* de que todo lo comunicado es secreto para terceros con independencia de cuál sea el contenido material de lo comunicado[27]; y el de la intimidad (artículo 18.1), que tiene un carácter material en la medida en que no se centra en el proceso de comunicación sino en el contenido de ésta, siendo esta última vertiente la que se ve protegida en el artículo 197.1.

B) BIEN JURÍDICO DEL APARTADO 2 DEL ARTÍCULO 197

El apartado 2 del artículo 197 castiga el apoderamiento, el acceso, la utilización y la modificación en perjuicio del titular de 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. Sanciona también el acceso, la utilización o la alteración de los ficheros que contienen tales datos en perjuicio del titular de los datos o de un tercero[28].

---

[25] La comunicación es, a efectos constitucionales, únicamente el proceso de transmisión de expresiones de sentido a través de cualquier conjunto de sonidos, señales o signos (STC 281/2006, de 9 de octubre) (STC 114/1984, de 29 de noviembre).

[26] RODRÍGUEZ LAINZ, 2011: 205.

[27] Afirma MARTÍN MORALES que este carácter formal del derecho al secreto de las comunicaciones favorece, indirectamente, la seguridad jurídica, en la medida en que en la práctica es difícil saber cuándo una carta es secreta porque el concepto de secreto es excesivamente elástico y seguramente la jurisprudencia no podría construir un criterio lo suficientemente seguro. MARTÍN MORALES, 1995: 40.

[28] Creo que el objeto material del segundo inciso son los ficheros y no los datos. Para más información véase Capítulo V.

La conducta prevista en el apartado 2 del artículo 197 tiene como bien jurídico la vertiente positiva del derecho a la intimidad[29], que garantiza al individuo un poder jurídico sobre la información relativa a su persona o a su familia, pudiendo imponer a terceros, sean éstos simples particulares o poderes públicos, su voluntad de no dar a conocer dicha información o prohibir su difusión no consentida[30]. El desarrollo de esta vertiente es, además, corolario evolutivo del desarrollo de la libertad informática[31], derecho a la protección de datos, *habeas data*[32] o derecho a la autodeterminación informativa[33], que puede definirse como el derecho del ciudadano a controlar sus datos personales frente a los múltiples riesgos de

---

[29] Al igual que sucede con todos los derechos fundamentales clásicos, la intimidad, originariamente configurada como un derecho de contenido negativo, progresivamente se transforma en una libertad de carácter positivo, concibiéndose como el presupuesto para el ejercicio de otros derechos fundamentales y ampliando su contenido al control de la información personal. ÁLVAREZ VIZCAYA, 2002: 2. CARBONELL MATEU y GONZÁLEZ CUSSAC, 2010: 995 (edición 1996) REVISAR. GALÁN MUÑOZ, 2013: 12. GONZÁLEZ RUS, 2011: 299. GRIMALT SERVERA, 2007: 31. MATA Y MARTÍN, 2001: 132. MUÑOZ CONDE, 2010: 270. PUENTE ABA, 2007: 165. RUEDA MARTÍN, 2004: 30-31. TOMÁS - VALIENTE LANUZA, 2010: 794.

[30] GARCÍA GARCÍA, 2003: 187.

[31] Para más información véase mi artículo MONTSERRAT SÁNCHEZ-ESCRIBANO, 2014: 1 y ss.

[32] Si bien en Derecho penal la protección de los datos se ha llevado a cabo desde la perspectiva de la intimidad, en los ámbitos constitucional y civil se configura como un derecho autónomo. El surgimiento de este derecho trata de combatir, en palabras de ALDAMA BAQUEDANO, la tendencia que hoy día existe dentro de las sociedades modernas a obtener el modelo de ciudadano transparente, que de lograrse dejaría reducido a unos niveles de mínimo extremo el concepto de intimidad y aún menor el jurídicamente protegible. ALDAMA BAQUEDANO, 1993: 16. BONILLA SÁNCHEZ, 2010: 209. MURILLO DE LA CUEVA, 1991: 96. MURILLO DE LA CUEVA, 2009: 15-16. MENÉNDEZ, 1994: 194. ORTÍ VALLEJO, 1994: 51. GRIMALT SERVERA, 1997: 156. MADRID CONESA, 1984: 30-33, 59, 60. ROVIRA VIÑAS, 1992: 260. RUIZ MIGUEL, 1995: 94. SÁNCHEZ BRAVO, 1998: 63. STEINMÜLLER et al., 1971 y 1972: 1-224. TONIATTI, 1991: 142. OLIVER LALANA, 2002: 1 y ss.

[33] DE DOMINGO, 2001: 280. JAREÑO LEAL, 1999: 1-7. MORALES PRATS, 2011a: 449 y 462. PÉREZ LUÑO 36-45. RODRÍGUEZ RUIZ, 1998: 14-20. RUIZ MIGUEL, 1995: 77.

conocimiento y utilización no consentidos generados como consecuencia de su tratamiento informatizado[34].

Nuevamente parece protegerse *a priori* ese otro derecho, en este caso el derecho a la protección de datos personales. Sin embargo, como muy bien indica su definición, en sede de constitucional el poder de control y disposición sobre los datos personales no solo engloba los datos íntimos sino que abarca cualquier dato que guarde relación con la personalidad, esto es, todos aquellos que identifiquen o permitan la identificación de la persona o que sirvan para cualquier otra utilidad que en determinadas circunstancias constituyan una amenaza para el individuo[35].

En cambio, en el ámbito penal la vulneración del bien jurídico protegido queda circunscrita únicamente a aquellos que, además de ser personales, cumplan dos condiciones[36]: ser *reservados* y tener un

---

[34] TOMÁS - VALIENTE LANUZA, 2010: 794.

[35] El concepto de datos de carácter personal aparece definido en el artículo 3 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, que los define como cualquier información concerniente a personas físicas identificadas o identificables. El Reglamento de desarrollo de dicha Ley complementa en el artículo 5.1 f) este concepto especificando que se trata de cualquier información numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo concerniente a personas físicas identificadas o identificables. El artículo 5.1 o) considera identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, mediante cualquier información referida a su identidad física, fisiológica, psíquica, económica, cultural o social. El apoyo constitucional de este derecho se encuentra en el artículo 18.4 de la Constitución que garantiza no solo la esfera más íntima o privada de las personas, sino también otros valores y libertades materializándose en una dimensión institucional basada en la configuración de facultades específicas de control sobre los datos. Para más información véase DE VERDA Y BEAMONTE, 2007: 123. DAVARA RODRÍGUEZ, 2003: 14. GARRIGA DOMÍNGUEZ, 1999: 127. ESTADELLA YUSTE, 1995: 32. HEREDERO HIGUERAS, 1996: 71. HERRÁN ORTIZ, 1999: 142. HERRÁN ORTIZ, 2003: 17. MURILLO DE LA CUEVA, 1993: 27. PIÑAR MAÑAS, 2010: 193-212. TÉLLEZ AGUILERA, 2001: 113-114.

[36] JAREÑO LEAL, quien se adhiere todavía a una concepción material mucho más restrictiva, distinguiendo entre datos reservados de carácter íntimo y datos reservados no íntimos. Para la autora, únicamente los datos reservados de carácter íntimo quedarían abarcados por la esfera de protección del artículo 197.2 del Código penal, mientras que los restantes serían objeto de sanción administrativa o civil. JAREÑO LEAL, 2008: 23, 63 y ss.

carácter personal o familiar. De ello se desprende que es únicamente la intimidad el único bien jurídico protegido en este delito[37].

En realidad el objeto de la intimidad es la información, es decir, datos sobre personas de carácter reservado que afectan a su esfera personal o familiar[38]. Así pues, la conducta típica pretende evitar la divulgación incontrolada por terceros de ciertos datos[39], cuya cesión ha sido realizada por el titular como consecuencia de un deber legal o del ejercicio muy concreto de un derecho y cuyo conocimiento supondría una injerencia en la zona espiritual o sustentadora de los elementos diferenciales del individuo[40]. Se trata, pues, de los datos relativos a la vida privada y familiar de la persona que ésta habría excluido del conocimiento público si no hubiera tenido que cederlos[41]. El objeto de estos datos es la intimidad y, este derecho es el único bien jurídico protegido en el tipo penal.

---

[37] CORCOY BIDASOLO señala que *[n]o puede olvidarse que la informática es un instrumento idóneo para cambiar o incorporar nuevas modalidades de conductas que atentan contra la intimidad e, incluso, facilitar los ataques.* A juicio de la autora, *[e]llo puede justificar una regulación específica, incluso en el ámbito penal, pero no la autonomía del bien jurídico protegido*, pues *esta pretendida autonomía sólo serviría para dificultar la protección o formalizarla.* CORCOY BIDASOLO, 2007: 13.

[38] MIERES MIERES, 2002: 57.

[39] La doctrina entiende que la clave de este precepto se halla no tanto en vulnerar la intimidad como en acceder ilegítimamente a ella, hecho que supone una derivación hacia una concepción formal de la intimidad como bien jurídico protegido, ya que a la concepción negativa del derecho a la intimidad como facultad de exclusión de terceros se ha visto completada por este aspecto positivo en tanto poder de control y disposición sobre la información. No comparte la afirmación de cierto sector de la doctrina como DE DOMINGO en relación a que ya no pertenece a la intimidad lo que se contiene en archivos y registros públicos, puesto que de hecho ya ha trascendido, y puede ser conocido. Para mí, tales datos continúan formando parte de la intimidad. MARTÍN MORALES, 1995: 33. MURILLO DE LA CUEVA, 1991: 84. JAREÑO LEAL, 1999: 15. MARCHENA GÓMEZ, 2001: 1099. ORTS BERENGUER y ROIG TORRES, 2001: 23. SOTO NIETO, 2004: 3 de 6. SOTO NIETO, 2001: 3-4.

[40] REBOLLO DELGADO, 2000: 49.

[41] CARBONELL MATEU y GONZÁLEZ CUSSAC, 2010:. RUEDA MARTÍN, 2004: 30, 73.

II. BIEN JURÍDICO EN EL DEROGADO ARTÍCULO 197.3

Como he señalado anteriormente, la Ley Orgánica 5/2010, de 22 de junio, introdujo el acceso ilícito en el apartado 3 del artículo 197 mediante la formulación de un tipo de equivalencia con el delito de descubrimiento y revelación de secretos. Fijada la intimidad como bien jurídico protegido en este último, queda ahora analizar si ésta ha de ser también el interés a tutelar en el apartado 3. Pues bien, al respecto cabe decir que el legislador, a través de la reforma de 2010, —la cual estuvo en vigor como cabe recordar desde 2010 hasta 2015[42]—, extendió incorrectamente el ámbito de tutela del precepto más allá de la intimidad, concretamente a la privacidad de la persona. A favor de esta tesis jugaban dos argumentos: la técnica de tipificación escogida por el legislador y la ubicación sistemática del precepto. Teniendo en cuenta tales circunstancias, a los efectos de reconducir la esfera de protección del precepto y delimitar adecuadamente el ámbito típico se convierte en imprescindible la interpretación teleológica del precepto para evitar un alejamiento excesivo de los tipos previstos en los dos primeros apartados —los tipos básicos— del artículo 197.

---

[42] Hasta la reforma del 2010, el artículo 197, que recoge los distintos tipos básicos del delito, venía a conformarse únicamente por dos conductas típicas con idéntica pena (prisión de 1 a 4 años y multa de 12 a 24 meses): el apartado 1, que castiga a quien, *para descubrir los secretos o vulnerar la intimidad de otro, sin su consentimiento, se apodere de sus papeles, cartas, mensajes de correo electrónico o cualesquiera otros documentos o efectos personales o intercepte sus telecomunicaciones o utilice artificios técnicos de escucha, transmisión, grabación o reproducción del sonido o de la imagen, o de cualquier otra señal de comunicación*; y el apartado 2, que sanciona *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*. Tras la reforma operada por la Ley Orgánica 5/2010, a estas dos conductas debe añadirse el nuevo apartado 3 que establece una pena inferior (prisión de 6 meses a 2 años) para quien *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*.

A) CONFIGURACIÓN COMO UN TIPO RESIDUAL

1. VÍA DE TIPIFICACIÓN ESCOGIDA POR EL LEGISLADOR

Como se ha indicado, para la incriminación del delito de acceso ilícito el legislador no optó primigeniamente por la creación de un tipo autónomo, sino de un tipo de equivalencia en relación con el delito de descubrimiento y revelación de secretos. Concretamente, para la construcción jurídica del tipo tomó como punto de referencia los dos tipos básicos previstos en el artículo 197.1 y .2. Dicha opción fue elegida por el legislador aun cuando no era la única vía posible, lo que impedía en buena medida afirmar que el bien jurídico protegido en el apartado 3 pudiera alejarse del interés tutelado en éstos, es decir, la intimidad[43].

---

[43] La reforma a nivel comparado que han afrontado los Estados para tipificar los distintos delitos vinculados a la informática se ha llevado a cabo a través de tres técnicas normativas:

> **a) Aprobación de leyes especiales:** aprobar leyes específicas y con un contenido puramente dedicado a los delitos que se han venido a denominar informáticos. Éste es el caso de Francia, Gran Bretaña, Holanda o Estados Unidos, por ejemplo.
> **b) Creación de tipos de equivalencia:** introducir nuevos tipos penales que complementen a los que ya existen y corrijan la descripción de la acción típica de tal forma que permitan subsumir las nuevas conductas vinculadas a la informática. Así, Italia, Portugal, Austria y España.
> **c) Creación de tipos *ex novo*:** crear nuevos tipos en los que incorporar la descripción de conductas normalmente peligrosas para el correcto funcionamiento de los sistemas informáticos y sus distintos componentes, protegiendo a aquél y a éstos con base en la potencialidad de producir una lesión a ciertos bienes jurídicos.

ROMEO CASABONA se decanta por lo que respecta al Estado español por el segundo sistema de incriminación, la introducción de tipos de equivalencia. Según el autor, esta técnica presenta la ventaja de concreción del tipo y vinculación de bienes jurídicos merecedores de protección penal muy bien perfilados, lo que es estimable en aras de la seguridad jurídica; pero su contrapartida consiste en que es fácil incurrir en excesivo casuismo o prolijidad, a la vez que se corre el riesgo de dejar sin cobertura determinadas conductas dignas de la intervención penal y otras nuevas que se pongan en práctica al hilo de los constantes avances tecnológicos en este sector. En cambio, opina que la creación de tipos *ex novo*, junto con la ventaja de asegurar una amplia cobertura penal frente a conductas indeseables, presenta el inconveniente de la pérdida de perspectiva de los bienes jurídicos que se desean proteger y de conferir una protección tal vez excesiva en este campo, lo que supone, respectivamente, riesgos para la seguridad jurídica y la posibilidad de sobrepasar el principio de intervención mínima. ROMEO CASABONA, 2003a: online. En similar sentido, RODRÍGUEZ GÓMEZ, 2003: 143.

2. UBICACIÓN SISTEMÁTICA DEL DELITO

Debido a que el apartado 3 se introdujo, en los términos comentados, en el seno del delito de descubrimiento y revelación de secretos, el legislador modificó el objeto material del delito, variando con ello el resto de elementos típicos. Así pues, fueron los datos y programas informáticos contenidos en el sistema informático el objeto material del delito y no el sistema informático, tal y como estaba previsto en la normativa supranacional.

Teniendo en cuenta que los datos informáticos eran también el objeto material de los dos apartados precedentes, cabía concluir la existencia de una coincidencia casi plena entre el objeto material del apartado 3 y los de los apartados 1 y 2:

> a) En el apartado 1 se protegen de los documentos electrónicos y mensajes de correo electrónico.
>
> b) En el apartado 2, los datos reservados de carácter personal o familiar contenidos en ficheros o registros públicos o privados.
>
> c) En el apartado 3, cualquier dato contenido en un sistema informático, característica predicable también de los datos a los que hace referencia tanto el apartado 1 como los el apartado 2.

Por consiguiente, para conseguir la equivalencia a la que se ha hecho referencia, en realidad lo que hizo el legislador español fue configurar el acceso ilícito como un complemento de los dos tipos básicos que le precedían, convirtiéndolo éste en un tipo residual que castigaba aquellos accesos a datos desprovistos de protección conforme a los dos apartados anteriores. De esta manera, la relación entre la nueva conducta y los dos tipos recogidos en los apartados .1 y .2 del Código penal se articulaba de la siguiente forma[44]:

---

[44] Un esquema similar en RUEDA MARTÍN, 2010:.

a) El acceso a datos informáticos para descubrir un secreto o vulnerar la intimidad de otro se sancionaba *ex* artículo 197.1.

b) El acceso a datos informáticos contenidos en un registro o un archivo de datos reservados de carácter personal o familiar en perjuicio del titular de los datos o de un tercero, se castigaba conforme al artículo 197.2.

c) El acceso a datos informáticos que no integrasen un supuesto subsumible en alguno de los anteriores tipos penales era constitutivo de un delito tipificado en el artículo 197.3.

En definitiva, el legislador español previó idénticas conductas a las recogidas en los apartados anteriores, pero ampliando el conjunto de datos que éstos protegían a supuestos que no estaban incluidos en su ámbito de aplicación[45]. De esta forma, la aplicación del nuevo apartado 3 del artículo 197 debía realizarse por exclusión de los demás apartados[46], constituyendo un cajón de sastre conforme al cual castigar todas las conductas no susceptibles de ser subsumidas en los dos apartados que le precedían[47] e integrando con ellos un concurso de normas a resolver por las reglas del artículo 8, concretamente por el principio de especialidad, a favor de los apartados .1 y .2[48].

---

[45] DE LA MATA BARRANCO y HERNÁNDEZ DÍAZ, 2010: 177.

[46] Resultaba, pues, indiferente en la aplicación del apartado tercero la existencia de un elemento subjetivo dirigido a causar un perjuicio, tal y como se manifestaba por una parte de la doctrina al diferenciar ambos apartados, pues su concurrencia en la conducta carecía de relevancia penal a tales efectos. Sería simplemente el distinto carácter de los datos la nota que impedía la aplicación del apartado 2. Véase para una exposición más completa y detallada CARRASCO ANDRINO, 2010a: 251.

[47] DE LA MATA BARRANCO, 2010: 177.

[48] Para más información sobre este particular véase Capítulo V, Sección 1ª, relativo al objeto material del delito.

3. IMPOSIBILIDAD DE DESLINDE RESPECTO DEL APARTADO 2 DEL ARTÍCULO 197

SÁNCHEZ DOMINGO añadía a las anteriores razones lo que vendría a constituir una tercera inconveniencia: la imposibilidad de deslindar el artículo 197.3 del artículo 197.2[49], como, de hecho, en su día ya planteó el Informe del Consejo General del Poder Judicial al Anteproyecto de Ley de 2008[50]. La autora consideraba que en el artículo 197.3 se castigaba meramente el acceso a datos reservados o de carácter personal o familiar al igual que lo hacía el apartado segundo del mismo precepto. Sin embargo, como puede desprenderse del correspondiente Capítulo[51], ello era sólo parcialmente cierto, ya que por una parte, los datos a los que hacía referencia el apartado 3 del artículo 197 eran los contenidos en el apartado 2, y, por otra, como he indicado, la colisión entre uno y otro hallaba solución conforme a las reglas de resolución de conflictos entre normas que ofrece el artículo 8 del Código penal.

[49] SÁNCHEZ DOMINGO, 2012: 27, 31.

[50] CGPJ, 2008

[51] Véase Capítulo V.

B) INDEBIDA EXTENSIÓN DEL ÁMBITO TÍPICO: NECESIDAD DE INTERPRETACIÓN TELEOLÓGICA DEL TIPO

Como tipo residual del delito de descubrimiento y revelación de secretos, el apartado 3 del artículo 197 no sólo permitía rellenar las lagunas de los apartados 1 y 2, sino también entender englobados todos aquellos supuestos que no se hallaban penados por éstos y que afectaran a datos informáticos. La razón de lo anterior estribaba en el hecho de que la única nota que se predicaba de los datos que protegía el apartado 3 era que se tratara de datos contenidos en todo o en parte de un sistema informático.

Lo anterior, de inicio, conducía a forzar indebidamente el bien jurídico para extender la protección penal a aquellos otros datos que, sin estar directamente referidos al ámbito estrictamente íntimo del sujeto en cuestión, o a su familia, se contuviesen dentro de uno de sus bienes: su sistema informático. A tal efecto, podrían incluso entenderse incluidos aquellos datos que no afectaran directamente a información íntima, como, por ejemplo, los de carácter económico, cuya tutela en sede de intimidad o privacidad ha sido expresamente excluida por el Tribunal Constitucional[52].

---

[52] En este mismo Sentido se pronuncia la Sentencia de la Audiencia Provincial de Vizcaya (Sección 2ª) número 90307 de 23 julio de 2014, en cuyo Fundamento Jurídico 4º afirma que en este delito no es *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.* A favor de este entendimiento se muestra también el hecho de que el acceso ilícito no debe ser realizado con ánimo de vulnerar la intimidad de otro o causarle un perjuicio -tal y como requieren los tipos de los apartados 1 y 2 del artículo 197- ya que el delito de acceso ilícito se consuma con el simple acceso o mantenimiento en el sistema tras vulnerar medidas de seguridad. Lo que demuestra que el objeto inmediato de tutela no es la intimidad, sino la seguridad e indemnidad del propio sistema que debe protegerse frente a posibles injerencias de terceros no autorizadas, con independencia de la naturaleza y contenido de los datos en él contenidos. A esto se añade que una interpretación del bien jurídico desde la perspectiva de la intimidad es desaconsejable, primero, porque plantearía problemas a la hora de delimitar algunos elementos del tipo como son los datos y, especialmente, los programas informáticos, que poco o nada tienen que ver con aquélla (CARRASCO ANDRINO, MATELLANES RODRÍGUEZ). Piénsese en este sentido que muchos datos incluido en un sistema informático puede no tener carácter personal: un trabajo académico, un archivo de música o un mero listado de celebraciones familiares (MATELLANES RODRÍGUEZ). Y segundo, porque la intimidad no es un bien jurídico predicable de las personas jurídicas, que también pueden ser titulares de un sistema informático (MOYA FUENTES).

La única forma de paliar esta expansión desmesurada del tipo penal era la realización de una interpretación teleológica del tipo[53] conforme a la propia sistemática del mismo en el marco del delito de descubrimiento y revelación de secretos[54]. Lo anterior suponía, de un lado, interpretar restrictivamente el tipo conforme al bien jurídico protegido en el delito que le daba cobijo, el descubrimiento y revelación de secretos; de otro, implicaba realizar una interpretación lo más extensiva posible del tipo vinculada a la literalidad de la norma pero respetando su fin de protección. Estas dos ideas serán las que se presenten a continuación.

1. RESTRICCIÓN DEL ÁMBITO APLICATIVO DEL PRECEPTO CONFORME AL BIEN JURÍDICO INTIMIDAD

Dotar de contenido al apartado 3 del artículo 197 y adaptarlo al fin de protección de la norma para establecer el alcance de la prohibición exigía necesariamente excluir la tutela de aquellos datos que no tuvieran una vinculación directa con el bien jurídico protegido: la intimidad. La intimidad, por tanto, debía actuar, en mi opinión, como criterio rector de los distintos supuestos subsumibles en el tipo, limitando la literalidad del precepto a aquellos que supusieran únicamente una afectación de la misma. Ello permitía englobar todos aquellos comportamientos ilícitos vulneradores de este derecho que todavía no hallasen protección penal y también incluso reconducir aquellas conductas de escaso desvalor penadas en los apartados 1 y 2 en las que era aconsejable la imposición de una pena menor a la prevista en los artículos 197.1 y .2.

---

[53] Como afirma TRAPERO BARREALES el esclarecimiento de qué bien jurídico merece ser penalmente protegido y la forma en cómo ha de establecerse su protección y garantía ha de tener lugar a través de la interpretación teleológico - valorativa más acertada para ese concreto tipo penal. Así, el bien jurídico debe ejercer su función de guía de la interpretación del nuevo tipos penal, de tal forma que permita excluir de la subsunción en la infracción de todos aquellos comportamientos que no la pongan en peligro. TRAPERO BARREALES, 2006: 69.

[54] Resaltando también que no podía pretenderse que el artículo 197.3 pasara a asumir funciones de protección que no le eran propias desde un punto de vista teleológico. MORALES PRATS, 2011b: 821.

2. POSIBILIDAD DE EXTENSIÓN DEL ÁMBITO APLICATIVO DEL PRECEPTO A LA PRIVACIDAD

Interpretando la norma conforme al bien jurídico intimidad, se concluía que la redacción del apartado 3 seguía siendo tan amplia que lo que hacía era extender la punición de los apartados 1 y 2 del artículo 197 a todos los supuestos que vulneraran bien jurídico. Ello suponía ofrecer protección de carácter absoluto a la intimidad, lo que generaba dudas en relación con el principio de intervención mínima o *ultima ratio*[55].

La redacción del tipo era tan amplia que resultaba posible extender el tipo penal más allá de dicha interpretación, aproximándose más a la idea de privacidad que de intimidad, permitiendo entender englobados en el tipo las conductas atentatorias contra otros tipos de datos, como los de carácter económico, comercial o interrelacional[56].

---

[55] Afirma en este sentido SOLA RECHE que la protección meramente fragmentaria del derecho a la intimidad encuentra justificación en la imposibilidad de abarcar mediante la descripción del tipo penal a todas las facetas que representa el derecho a la intimidad en el acontecer de la vida y de las relaciones humanas. A ello se añade el recordatorio de la doctrina de que únicamente deben ser objeto de protección las manifestaciones del derecho a la intimidad con mayor relevancia para las personas y, además, sólo frente a las agresiones más intolerables contra ellas. Por este motivo, las demás vulneraciones de este derecho deberán ser castigadas mediante sanciones de índole civil. Véase SOLA RECHE, 1991: 193-194. E, igualmente, ROMEO CASABONA, 2004b: 30, ROMEO CASABONA, 2003b: 515. ORTS BERENGUER y ROIG TORRES, 2001: 19.

[56] Para ANARTE BORRALLO y DOVAL PAIS la norma adelantaba el umbral típico hasta incorporar estadios previos, lo que convierte el precepto en una figura de peligro abstracto. Así, pues, consideraban que el número 3 del artículo 197 suponía un adelantamiento de la protección en un doble sentido:

> a) primero, porque permitía sancionar hechos que representasen riesgos para la intimidad y los datos personales.
>
> b) segundo, porque permitía sancionar hechos dirigidos a descubrir y/o revelar la intimidad o los datos personales.

ANARTE BORRALLO y DOVAL PAÍS, 2012: 14-15.

La noción de privacidad[57] tiene un origen anglosajón[58]. La mayor parte de la doctrina entiende que se trata de un concepto con un contenido más amplio que la intimidad[59], siendo utilizado frecuentemente por el Tribunal Constitucional e, incluso, por el Tribunal Europeo de los Derechos Humanos como un concepto globalizador de los distintos derechos que integran la personalidad, pero no sustitutivo de cada uno de ellos. No obstante, todavía pueden leerse trabajos en los que se defiende una interpretación

---

[57] Aun a pesar del carácter expreso del Código penal en cuanto a la mención del derecho a la intimidad en la propia rúbrica del Título X, cierto sector doctrinal aboga por adoptar un concepto amplio de intimidad, concibiéndolo como sinónimo del de privacidad. Sin embargo, sin entrar en este momento a pronunciarme en torno al debate doctrinal suscitado respecto de la aceptación de la translación de dicho derecho -algo, a mi juicio, innegable- a nuestro ordenamiento jurídico, es necesario poner de relieve en contra de dichos autores que la mayor parte de la doctrina concibe la privacidad y la intimidad como conceptos distintos aunque conectados entre sí, y entiende que es ésta última la que debe ser erigida como bien jurídico protegido en el delito de descubrimiento y revelación de secretos. Esta postura es, en mi opinión, la más coherente con el principio de *ultima ratio* que rige en Derecho penal y, por tanto, este estudio se adhiere a la opinión de aquellos autores que limitan el contenido del bien jurídico a la intimidad en su sentido más restringido. Recogiendo estas posturas, mientras que autores como DAVARA RODRÍGUEZ, MORALES PRATS, MARCHENA GÓMEZ, este último con una concepción mucho más radical que postula incluso la superación de la concepción de la intimidad como derecho, o RUIZ MIGUEL, MARTÍN-CASALLO LÓPEZ, abogan por ampliar el campo de protección del individuo especialmente como consecuencia de la posición que éste ocupa en la sociedad tecnológica. También aboga por un concepto amplio LÓPEZ DÍAZ, 1996: 186. Por el contrario, otro sector de la doctrina considera que la privacy no tiene cabida en nuestro derecho o bien que la privacidad como traducción del concepto privacy anglosajón no es sino una noción sinónima al derecho a la intimidad. En tal sentido opina, por ejemplo, SÁNCHEZ BRAVO, ORTÍ VALLEJO. Véanse también MORALES PRATS, 1984: MIRAR. MARCHENA GÓMEZ, 1996: 9-10. SÁNCHEZ BRAVO, 1998: 63.

[58] Es una cita comúnmente extendida y da la impresión casi obligada de que cuando se hace referencia a la privacy como concepto de origen anglosajón recordar a la primera formulación de este derecho como *the right to be left alone,* por parte de Warren y Brandeis. BRANDEIS y WARREN, 1890: 1 y ss.

[59] Esta es, de hecho, la opción por la que optó la Ley Orgánica 5/1992, de Regulación del Tratamiento Automatizado de Datos, que en su Exposición de Motivos afirmaba que *aquella, la privacidad, es más amplia que ésta, intimidad, pues en tanto la intimidad protege la esfera en que se desarrollan las facetas más singularmente reservadas de la vida de la persona -el domicilio donde realiza su vida cotidiana, las comunicaciones en las que expresa sus sentimientos, por ejemplo-, la privacidad constituye un conjunto, más amplio, más global de facetas de su personalidad que aisladamente consideradas, pueden carecer de significación intrínseca pero que, coherentemente enlazadas entre sí, arrojan como precipitado un retrato de la personalidad del individuo que éste tiene derecho a mantener reservado.*

amplia del concepto de intimidad, sustituyendo casi la noción mantenida en el presente estudio de intimidad por la de privacidad[60].

Sin atender en este momento al debate doctrinal suscitado en torno a la aceptación de la traslación de dicho derecho —algo, a mi

[60] Mientras unos autores mantienen una cierta separación entre derechos fundamentales de los apartados 1 y 3 del artículo 18, otros creen más apropiado concebirlos como manifestaciones de la privacy. La causa de estas diferencias doctrinales estriba en que el tratamiento de la intimidad en nuestra Constitución, al igual que ocurre con la libertad, es fragmentario. En este sentido, cierto sector de la doctrina ha resaltado que poco a poco el contenido del derecho a la intimidad se va ampliando y acercando cada vez más a una acepción amplia de vida privada, entendido como un espacio físico y espiritual reservado al ser humano necesario para que éste pueda excluirse del resto de la sociedad, pudiendo decidir dentro del ámbito de su libertad quién puede entrar en él y, a la vez, se trata de un espacio en el que puede desarrollar todas sus potencialidades como persona sin la injerencia injustificada de terceros, y alejándose de la restrictiva acepción vida íntima, como idea de secreto. DAVARA RODRÍGUEZ entiende que la protección de los datos personales está suficientemente protegida, en las modernas legislaciones, mediante el derecho a la intimidad. Es cuando surge la informática, y la posibilidad de tratamiento automatizado de la información y su transmisión telemática cuando aparece una nueva relación entre datos y personas que necesita ser protegida más allá de las normas referentes a la intimidad. El derecho que se trata de proteger no es solamente el derecho a la intimidad, sino algo con mayor profundidad que, en los ordenamientos de ámbito anglosajón, se ha dado en llamar privacy y que nosotros hemos traducido por privacidad En este sentido, DE DOMINGO, quien reconoce en primer lugar la distinción entre ambos conceptos, indica que si no se admitiera una interpretación amplia del derecho a la intimidad, habría casos en los que la persona ofendida no hallaría ningún derecho fundamental en el que sustentar su defensa, lo que sería preocupante, pues puede tratarse de situaciones especialmente lesivas para una persona. Por su parte, RUIZ MIGUEL cree que el entendimiento del derecho a la intimidad en un sentido amplio ofrece una categoría lo suficientemente flexible como para brindar una protección del más alto rango frente a ataques que puedan surgir por nuevos avances de la técnica que, en principio, son imprevistos para el legislador DE DOMINGO, 2001: 301. GRIMALT SERVERA, 2007: 36. REBOLLO DELGADO, 2000: 86. MURILLO DE LA CUEVA, 1991: 1 y ss. RUIZ MIGUEL, 1995: 29. MARTÍN MORALES, 1995: 35. BOIX REIG, 1989: 19. GARCÍA GUERRERO, 2013: 486. RODRÍGUEZ LAINZ, 2011: 205.

juicio, innegable— a nuestro ordenamiento jurídico[61], la mayor parte de la doctrina concibe la privacidad y la intimidad como conceptos distintos aunque conectados entre sí, y entiende que es ésta última la que debe ser erigida como bien jurídico protegido. Para estos autores, lo íntimo sería un concepto estricto de dimensiones propiamente individuales y lo privado sería un ámbito que, abarcando lo íntimo, lo supera[62]. Así las cosas, por su amplitud debía interpretarse que el ámbito de aplicación del delito que tipificaba el artículo 197.3, quedase proyectado a aquellas conductas que potencialmente pudiesen llegar a afectar a la privacidad de las personas[63].

---

[61] Así, mientras que autores como DAVARA RODRÍGUEZ, MORALES PRATS, MARCHENA GÓMEZ, este último con una concepción mucho más radical que postula incluso la superación de la concepción de la intimidad como derecho, o RUIZ MIGUEL, MARTÍN-CASALLO LÓPEZ, abogan por ampliar el campo de protección del individuo especialmente como consecuencia de la posición que éste ocupa en la sociedad tecnológica. Por el contrario, otro sector de la doctrina considera que la privacy no tiene cabida en nuestro derecho o bien que la privacidad como traducción del concepto privacy anglosajón no es sino una noción sinónima al derecho a la intimidad. En tal sentido opina, por ejemplo, SÁNCHEZ BRAVO, ORTÍ VALLEJO. Véanse también MORALES PRATS, 1984: 128 y 129. MARCHENA GÓMEZ, 1996: 9 y 10. SÁNCHEZ BRAVO, 1998: 63.

[62] La intimidad así entendida aparece integrada por aquellas manifestaciones de la personalidad individual o familiar cuyo conocimiento o desarrollo quedan reservados por su titular o sobre las que ejerce alguna forma de control cuando se ven implicados terceros, entendiendo por tales tanto los particulares como los poderes públicos. La privacidad, por su parte, integraría el conjunto de facetas vinculadas a la personalidad que pueden ser identificadas como manifestaciones de la vida privada. REBOLLO DELGADO, 2000: 88. RUIZ MIGUEL, 1995: 29. ROMEO CASABONA, 2006b: 174.

[63] De esta manera, debe interpretarse que el delito previsto en el artículo 197.3 se endereza a la protección de la seguridad de los sistemas informáticos, pero teniendo como fin último a la preservación de la privacy informática de las personas MORALES PRATS, 2011b: 822.

SECCIÓN 2ª

ANÁLISIS DEL BIEN JURÍDICO PROTEGIDO EN EL ARTÍCULO 197.1 *BIS*

I. INTRODUCCIÓN

El artículo 197.3 al que se ha hecho referencia fue uno de los puntos objeto de modificación por la reforma de la Ley Orgánica 1/2015, de 30 de marzo. Concretamente, fueron dos los cambios que se realizaron: el primero, la ubicación sistemática del precepto, el segundo, su literalidad.

> a) Por lo que respecta a la ubicación sistemática, el delito fue trasladado del apartado 3 del artículo 197 a al apartado 1 del artículo 197 *bis*, precepto de nueva creación por parte de la Ley Orgánica 1/2015. El acceso ilícito, por tanto, dejó de ser un tipo de equivalencia en relación con el descubrimiento y revelación de secretos para constituir un tipo autónomo pero manteniéndolo en el seno del mismo Capítulo. Por consiguiente, a día de hoy el delito de acceso ilícito a un sistema informático constituye un tipo con entidad propia dentro de los delitos de descubrimiento y revelación de secretos, estando recogido en el artículo 197.1 *bis* del Capítulo I del Título X del Libro II del Código penal, dedicado a los *Delitos contra la intimidad, la propia imagen y la inviolabilidad del domicilio*.
>
> b) En cuanto a la nueva redacción, la Ley Orgánica 1/2015, de 30 de junio, el delito de acceso ilícito ha sufrido una reestructuación por lo que respecta a sus elementos típicos. De entre las distintas modificaciones, la más sustancial ha sido la relativa al objeto material del delito, que es ahora el sistema informático.

Ambas modificaciones permiten desvincular el delito de acceso ilícito del derecho a la intimidad y reinterpretarlo conforme a nuevos parámetros. El problema se centra entonces en determinar cuál es el bien jurídico protegido en el nuevo tipo penal y en qué medida éste se encuentra vinculado al Título que da cobijo a la conducta.

II. LA INTIMIDAD COMO BIEN JURÍDICO

Como se ha anunciado, aunque la reforma operada por la Ley Orgánica 1/2015, de 30 de marzo, ha convertido el delito de acceso ilícito en un tipo autónomo, lo ha mantenido en el artículo 197.1 *bis*, dentro del mismo Capítulo I del Título X, relativo al *Descubrimiento y revelación de secretos*. Por este motivo, considero oportuno iniciar el comentario del bien jurídico protegido con la postura que defiende un interés más cercano a la ubicación sistemática del propio precepto: la intimidad. Y es que en el Código penal español este delito parece inamovible de entre los delitos contra intimidad, como si existiera un convencimiento manifiesto del legislador en que el interés tutelado es el mentado derecho. Ello presenta como inexcusable el análisis del tipo a la luz de la intimidad a los efectos de discernir su posible vinculación así como determinar la corrección de su ubicación sistemática.

A) POSTURAS A FAVOR DE LA INTIMIDAD

Incluso antes de la reforma de 2010, algunos autores apuntaron al derecho a la intimidad como bien jurídico protegido en el delito de acceso ilícito. Así, HUERTA TOCILDO y ANDRÉS DOMÍNGUEZ entendieron que el acceso a un sistema informático no puede tener un propósito distinto al de penetrar en la esfera íntima del titular de los datos contenidos en el mismo[64].

Aprobada la reforma de 2010, unos pocos autores sostuvieron también esta postura. Tras la reforma de 2015, en cambio, se ha vuelto todavía más minoritaria. Asimismo, dentro del sector doctrinal que defiende o ha defendido que es la intimidad el bien jurídico protegido puede distinguirse un triple enfoque:

[64] HUERTA TOCILDO y ANDRÉS DOMÍNGUEZ, 2002: 26.

a) Postura abierta: RAGUÉS I VALLÉS y ROBLES PLANAS, adoptan una posición muy abierta considerando cualquier acceso como un menoscabo de la intimidad[65].

b) Postura intermedia: MATELLANES RODRÍGUEZ, CORRIAS LUCENTE y POMANTE, en una posición intermedia, discriminan los ilícitos subsumibles en atención al contenido del sistema[66].

c) Postura restringida: esta postura va en la línea ya apuntada por HUERTA TOCILDO y ANDRÉS DOMÍNGUEZ, quienes entienden que el único ánimo que puede motivar al sujeto a cometer este delito es vulnerar la intimidad. Esta tesis, que va consolidándose cada vez más en la doctrina italiana, define la intimidad como el interés exclusivo del titular para disponer, gozar y controlar los datos e informaciones del sistema[67].

---

[65] RAGUÉS I VALLÉS y ROBLES PLANAS relativizan el comportamiento típico de una forma a mi juicio excesivamente laxa al considerar que el propio acceso ya supone la creación de un peligro para la intimidad, existiendo afectación del bien jurídico con independencia de que efectivamente el sujeto activo no llegue a obtener datos que formen parte del sistema informático incluso sin tener en cuenta la naturaleza o el contenido de dichos datos o programas. RAGUÉS I VALLÈS et al., 2012: 371. También CASTIÑEIRA PALOU y ESTRADA CUADRAS, 2015: 163.

[66] MATELLANES RODRÍGUEZ afirma que la vulneración del bien jurídico intimidad se produciría como consecuencia no sólo de una penetración en el sistema, sino de la captación de la información personal que se encuentra contenida en el propio sistema informático y que el titular de la misma no quiere poner a disposición de terceros. La obtención de información contenida en el sistema informático, cualquiera que fuera su contenido, sería pues el criterio de delimitación en este caso de la lesión al bien jurídico intimidad. CORRIAS LUCENTE, 2001: 499. MATELLANES RODRÍGUEZ, 2008: 62. POMANTE, 1999: 25-26. En igual sentido, LÓPEZ ORTEGA, 2004: 123. SÁNCHEZ DOMINGO, 2012: 29.

[67] Explica PECORELLA que se trata de una solución coherente con la experiencia criminológica de la cual emerge que el acceso abusivo a un sistema informático tiene como objetivo constantemente la adquisición indebida del material contenido en el sistema. A ello añade MANTOVANI que esta configuración del bien jurídico permite atender tanto a una función incriminatoria primaria, concretada en la punición de la indiscreción informática, cuanto a una función incriminatoria secundaria, dirigida al uso no autorizado del sistema informático ajeno. CERQUA, 2000: 53. MANTOVANI, 2011: 545. MERLI, 1993: 127. NUNZIATA, 1996: 44. PAZIENZA, 1995: 80. PECORELLA, 2011: 5980. PECORELLA, 2006: 335. TRENTACAPILLI, 2002: 1283-1286. MANTOVANI, 2011: 522. PECORELLA, 2006: 316. PECORELLA, 2011: 5980.

B) VALORACIÓN PERSONAL

Aunque opino que el bien jurídico protegido en el hoy derogado apartado 3 del artículo 197 era la intimidad, ello en nada obsta a que, por otra parte, considere que el Título X nunca debería haber dado cobijo a esta conducta y que, tras la nueva modificación operada por la Ley Orgánica 1/2015, de 30 de marzo, el bien jurídico sea distinto. Afirmar que el delito de acceso ilícito encaja en el seno de los tipos relativos al descubrimiento y revelación de secretos conduce a soslayar determinados aspectos de la configuración típica del mismo, además de una completa desvinculación de lo establecido en la normativa supranacional[68].

1. VINCULACIÓN ÚNICA A LA INTIMIDAD

Tipificar el acceso ilícito entre los delitos contra la intimidad supone vincular la conducta únicamente a este bien jurídico, lo que obliga a sobrentender que todos los datos y programas contenidos en un (cualquier) sistema informático pertenecen forzosamente a la esfera más íntima de la persona[69]. Esta premisa supone negar una realidad tan plausible como la existencia de sistemas informáticos con distinta finalidad a la de albergar datos íntimos, como pueden ser, a modo de ejemplo, los sistemas pertenecientes a una empresa o aquellos que se utilizan para trabajar y, por tanto, contienen datos protegidos por el derecho a la propiedad intelectual como la presente tesis doctoral.

Además aunque podría decirse que el Convenio sobre Cibercriminalidad prevé la posibilidad de que los Estados parte adicionen a la conducta un elemento subjetivo del injusto consistente en la intención de obtener datos, ello no significa que esta tendencia subjetiva del autor deba quedar vinculada únicamente al derecho a la intimidad.

---

[68] SÁNCHEZ DOMINGO, 2012: 27. FERNÁNDEZ TERUELO, 2011: 197.

[69] A favor, SÁNCHEZ DOMINGO, 2012: 31.

2. ACCESO ILÍCITO COMO BARRERA DE PROTECCIÓN

La incriminación del acceso ilícito responde a la necesidad de ofrecer protección a los usuarios legítimos de los sistemas y los datos contra las intromisiones en los sistemas informáticos que puedan conducir potencialmente a una ulterior comisión de ilícitos con un mayor contenido de injusto[70]. En este sentido, debería de haberse configurado como un tipo destinado a brindar protección al sistema de forma adicional a las posibles medidas de seguridad que el usuario hubiera instalado en una primera etapa contra tales peligros[71].

Desde la perspectiva apuntada, vincular el acceso ilícito únicamente a la intimidad supone soslayar también que la realización de dicho comportamiento puede poner en peligro no sólo la intimidad sino también ese otro conjunto de derechos respecto de los cuales el acceso ilícito pretende constituir una anticipación de la tutela punitiva y, por otra parte, —y esto incluye a la intimidad— no llegan a verse lesionados con la comisión de la conducta de acceso. De este modo, el delito de descubrimiento y revelación de secretos constituye tan solo uno de los tipos penales cuya protección quiere reforzarse a través de la incriminación del acceso ilícito[72], pero no el único, pues el delito de acceso ilícito tiene como misión ofrecer una protección mediata frente a ataques no deseados ta otros bienes jurídicos como el secreto de empresa, la propiedad intelectual, el patrimonio o la seguridad nacional[73].

---

[70] COUNCIL OF EUROPE, 2001: 13-14 párrafos 44-45.

[71] COUNCIL OF EUROPE, 2001: 13-14 párrafos 44-45.

[72] En este sentido, tal y como afirma MORALES PRATS, *si entendemos este nuevo delito de acceso ilícito a los sistemas informáticos como un adelantamiento a la intervención del Derecho penal frente a la criminalidad informática, lo lógico es considerar esta nueva figura delictiva desde su contenido y dimensión transversal, con lo que se trata de una previsión legal no solo al servicio de una protección adelantada de la intimidad sino también de otros bienes jurídicos de la misma naturaleza.* MORALES PRATS, 2011b: 820.

[73] Sobre el particular véase el apartado VII. E) de la Sección 2ª del presente Capítulo.

3. AUSENCIA DE ELEMENTO SUBJETIVO DEL INJUSTO

Igualmente, este delito constituye una *rara avis* en el marco de la protección penal de la intimidad[74] al carecer del elemento más importante que caracteriza a los tipos penales de este género y en el que se manifiesta la auténtica voluntad quebrantadora del bien jurídico por parte del autor: el elemento subjetivo del injusto. Al contrario, en el acceso ilícito a un sistema informático el sujeto activo no tiene la intención de atacar la intimidad, obtener datos íntimos ni, aun menos, causar un perjuicio[75]. No se trata, por tanto, de un delito mutilado de dos actos, pues no existe en este caso una finalidad posterior de revelación de los datos, con lo que quiebra el esquema básico de los delitos contra la intimidad contenidos hasta ahora en nuestro Código penal[76].

---

[74] ANARTE BORRALLO y DOVAL PAÍS, 2012: 12.

[75] En este sentido, la Sentencia del Tribunal Supremo 40/2016, de 3 de febrero, castiga por el apartado 3 y no el 2 el acceso por parte del exmarido al historial clínico de su ex-mujer sin intención de causarle un perjuicio (véase F. J. 2º).

[76] MORALES PRATS distingue entre actos de intrusión y actos de revelación como criterio ordenador de las distintas modalidades de ataque a la privacy. Así como el descubrimiento y revelación de secretos sería un delito de naturaleza compleja, integrado por dos accesiones, el acceso subrepticio, y la posterior revelación de los secretos, el acceso ilícito a datos informáticos tal y como se prevé en el artículo 197.3 del Código penal estaría conformado únicamente por un único acto, el acto de intrusión, de lo que se desprende que no es posible el encaje típico del acceso ilícito en los delitos contra la intimidad del artículo 197.1 y .2. En el artículo 197.1 porque la exigencia de un ánimo dirigido específicamente a descubrir los secretos o vulnerar la intimidad no concurre en el acceso ilícito, al igual que tampoco lo hace la finalidad de causar un perjuicio exigida en el apartado 2 del artículo 197 del Código penal. Esta estructura crea una divergencia total entre el delito de descubrimiento y revelación de secretos y la configuración efectuada del acceso ilícito, cuya naturaleza se ha marcado desprovista de cualquier elemento subjetivo del injusto. Por tanto, este delito quiebra en este aspecto el esquema básico de los delitos contra la intimidad contenidos hasta ahora en nuestro Código penal, en los que siempre tiene lugar ese ánimo específico que mueve la conducta del sujeto activo. Así, en el supuesto concreto de que el hacker acceda a los datos contenidos en un sistema informático por el simple hecho de mostrar el reto de poder vencer a las claves de acceso, vulnerando las medidas de seguridad establecidas para impedir dicho acceso o, en la hipótesis de que el hacker accede a un sistema informático con el reto de demostrar su pericia sin que se despierte en él ningún ánimo de conocer o descubrir los secretos contenidos en los datos o sistema al que accede. Sin embargo, el mero acceso al sistema vulnerando las medidas de seguridad ya supone consumar el delito de acceso ilícito. SÁNCHEZ DOMINGO, 2012: 31.

III. DOMICILIO INFORMÁTICO

A) CONCEPTO, NATURALEZA Y CONTENIDO ESENCIAL DEL DOMICILIO INFORMÁTICO COMO BIEN JURÍDICO

Siguiendo la tendencia iniciada por la Recomendación 89 (9), de 13 de septiembre, del Consejo de Europa, sobre delincuencia informática, un sector de la doctrina defiende que el bien jurídico protegido en el delito de acceso ilícito es el domicilio informático[77]. Esta tesis es la más extendida en Italia y es, de hecho, la que el propio legislador italiano ha reflejado en el artículo 615 *ter* del Código penal al ubicar la conducta en el Capítulo relativo al allanamiento de morada[78]. Asimismo, el paralelismo anunciado se manifiesta específicamente en un elemento de orden sistémico, la **estructura típica**, que se construye a imagen y semejanza de los delitos contra la inviolabilidad del domicilio, previéndose una modalidad activa, el acceso ilícito, y una pasiva, la de mantenimiento ilícito. Efectivamente, aunque el legislador español ha introducido el acceso ilícito en el Capítulo relativo al descubrimiento y revelación de secretos, ha importado esta doble vía de afectación del bien jurídico, siendo éste el principal argumento que permite a la doctrina vincular el artículo 197.1 *bis* al domicilio[79]. Pues bien, al igual que en el ámbito italiano los defensores de esta postura **equiparan** el sistema informático con el domicilio físico tradicional al considerarlo como una expansión del área de respeto perteneciente a la persona y en la que toda intromisión no deseada por el titular es considerada un allanamiento de la morada informática[80].

---

[77] El estudio pormenorizado del contenido de dicha norma se encuentra en el Epígrafe II del Capítulo I.

[78] Para más información sobre la regulación italiana véase el Capítulo II.

[79] Así, por ejemplo, MORALES GARCÍA, 2010: 28. Sobre el artículo 197.3: Sentencia de la Audiencia Provincial de Vizcaya (Sección 2ª) número 90307 de 23 julio de 2014, Fundamento Jurídico 4º.

[80] LEZERTÚA sienta su base en la vulneración del derecho al respeto de la vida privada consagrado en el artículo 8 del Convenio Europeo de los Derechos Humanos, destacando que su penalización autónoma tiene carácter preventivo en tanto en cuanto representa una especie de infracción básica a partir de la cual pueden cometerse otros delitos informáticos más graves. LEZERTÚA, 2002: 33-34.

Los partidarios de esta teoría conciben el domicilio informático como un **espacio ideal** de carácter inviolable donde se almacenan los datos informáticos de una o varias personas. Para estos autores tal inviolabilidad constituye, además, **manifestación directa del *ius excludendi*** del titular de los datos, esto es, la expresión de la voluntad de aquel en cuanto a ofrecer protección a estos últimos frente a cualquier tipo de intromisión no autorizada[81].

Por consiguiente, el derecho al domicilio informático tiene, según estos autores, una **naturaleza individual y puramente instrumental o formal**[82] concretada en otorgar al titular del sistema informático la facultad de mantener a éste y, sobre todo, a los datos y programas en él contenidos al margen de injerencias ajenas que pudieran conducir a ulteriores invasiones de la intimidad o, en menor medida, a la vulneración de otros derechos de la persona[83].

---

[81] En la doctrina italiana pueden distinguirse tres teorías en torno a la configuración del domicilio informático:

a) Domicilio informático como expansión del domicilio tradicional: entiende que los sistemas informáticos constituyen una expansión ideal del área de respeto perteneciente al sujeto interesado.

b) Espacio informático: entendido éste como el espacio inmaterial y no espacial informático del que puede disponer libremente el titular, sin intrusiones no deseadas.

c) Teoría mixta: otros autores aúnan ambos aspectos, el físico y el ideal, y definen el domicilio informático como el espacio físico e ideal de pertenencia de la esfera individual personal tutelada en la Constitución.

ALMA y PERRONI, 1997: 505. BORRUSO, 1994: 28. CARINGELLA et al., 2011: 1051. CUOMO, 2000: 2998. CUOMO y RAZZANTE, 2009: 96. DESTITO et al., 2007: 81, 83. FIANDANCA y MUSCO, 2013: 293. GALDIERI, 1996: 189. GALDIERI, 1997: 138. GAROFOLI, 2013: 639. GATTA, 2011: 300. MARANI, 2007: 613. MONACO, 2011: 2334. PARODI y CALICE, 2001: 64-65. PICA, 1999: 68. RELLA, 2007: 39.

[82] BORJA JIMÉNEZ señaló ya en su día respecto de la inviolabilidad del domicilio tradicional que no se está haciendo referencia al contenido del injusto del delito, sino mas bien a una referencia formal al bien jurídico, sin entrar todavía a determinar su contenido material. Y, aunque este derecho ha sido reconocido como un auténtico derecho fundamental de la persona, en realidad no significa que el domicilio no pueda ser lesionado, sino tan sólo que en principio se impide al poder estatal entrar en la esfera personal localizada contra la voluntad de su titular y que excepciones a este acceso solo están permitidas cuando se fundamental en una facultad o permiso jurídico constitucional. BORJA JIMÉNEZ, 1990: 77-78. BORJA JIMÉNEZ, 1997: 226-228.

[83] GALÁN MUÑOZ, 2009: 95-96.

El **contenido esencial** de este derecho supone, en consecuencia, concebir el sistema informático como un espacio de pertenencia exclusiva del titular, que almacena en él su información vital[84] y que manifiesta directamente mediante este mismo acto (el almacenamiento de la información para sí) su voluntad de reservar explícitamente el contenido del sistema frente a terceros como medio de preservación de su intimidad[85]. El sistema informático conforma, pues, para estos autores la expresión directa de la vida privada de una o varias personas que, en todo caso, debe quedar restringida al alcance de terceros[86]. La **afectación del bien jurídico** domicilio informático se produciría en este caso como consecuencia de la injerencia de un tercero en este reducto íntimo que constituiría el sistema informático.

En el ámbito español, son dos los autores españoles —y una sentencia[87]— que apuestan por esta nueva concepción informática del domicilio como bien jurídico: MORALES GARCÍA y GALÁN MUÑOZ[88]. Según estos autores, en el caso del acceso ilícito no se produce una afectación de un bien jurídico colectivo, sino únicamente de uno individual: la inviolabilidad informática del sistema que es accedido, interés muy próximo a otro de corte tradicional y eminentemente individual, la intimidad[89]. Así pues, en su opinión, se tutela a los sistemas informáticos con carácter individual en la medida en que contienen información sensible para la intimidad, hecho que, por otra parte, implica excluir de la protección del tipo delictivo la tutela de los sistemas informáticos en sí mismos considerados[90].

---

[84] MORALES GARCÍA, 2010: 28.

[85] MATELLANES RODRÍGUEZ, 2004: 185. MORALES GARCÍA, 2010: 28.

[86] MATELLANES RODRÍGUEZ, 2004: 185.

[87] Sobre el artículo 197.3: Sentencia de la Audiencia Provincial de Vizcaya (Sección 2ª) número 90307 de 23 julio de 2014, Fundamento Jurídico 4º.

[88] GALÁN MUÑOZ, 2009: 33.

[89] GALÁN MUÑOZ, 2009: 95-96.

[90] GALÁN MUÑOZ, 2009: 95-96.

B) VALORACIÓN PERSONAL

Defender que el bien jurídico protegido en el delito de acceso ilícito a un sistema informático es el domicilio informático implica, en mi opinión, constreñir excesivamente el injusto típico de éste excluyendo de su ámbito de aplicación un importante número de supuestos con idéntico o mayor desvalor. Particularmente, son tres las razones por las que esta concepción no resulta aplicable al tipo objeto de análisis: la estrecha vinculación existente entre domicilio e intimidad, la propia configuración del derecho a la inviolabilidad del domicilio sobre la base de la relación de la persona con el espacio físico y un argumento de menor peso, a saber, la ubicación sistemática del precepto.

1. EXCESIVA VINCULACIÓN CON LA INTIMIDAD

El principal inconveniente de mantener que el bien jurídico protegido es el domicilio informático se concreta en su estrecha vinculación con el derecho a la intimidad. Efectivamente, como se ha indicado, el contenido del derecho a la inviolabilidad domiciliaria informática viene determinado por la voluntad de reserva del titular de los datos y programas informáticos pertenecientes a la vida privada personal y familiar frente a su conocimiento por parte de terceros[91].

La idea apuntada constituye la traslación al ámbito informático de la noción tradicional de domicilio, que concibe a éste como la prolongación espacial de la voluntad del morador sobre el cual éste ostenta facultades de exclusión frente a terceros. Respecto de si la noción tradicional de domicilio existían serias dudas acerca de si el domicilio es un derecho con autonomía y entidad propia, pudiéndose diferenciar tres corrientes doctrinales al respecto:

---

[91] En los términos expuestos en la página 40 a 42.

a) Una primera corriente niega autonomía a la inviolabilidad del domicilio, entendiendo que es la intimidad el bien jurídico protegido en el delito de allanamiento de morada[92].

b) Una segunda postura perciben el domicilio como una emanación del derecho a la intimidad[93].

c) Finalmente, algunos autores que conciben el domicilio como un interés con autonomía propia, aun admitiendo la existencia de una estrecha vinculación existente entre éste y la intimidad.

---

[92] No es infrecuente señalar a la intimidad como bien jurídico protegido en el delito de allanamiento de morada. SANZ MORÁN pone de relieve que la inviolabilidad del domicilio no es el bien jurídico protegido en el delito y, además, afirma que la interpretación sistemática que se había realizado del domicilio en el ámbito constitucional llevó a poner en conexión la anterior declaración con a garantía del derecho a la intimidad personal y familiar del apartado 1 del artículo 18, de modo que la inviolabilidad del domicilio constituiría así una de las manifestaciones del derecho a la intimidad o, expresado en otros términos, la inviolabilidad del domicilio aparece como un instrumento de tutela de la intimidad. JORGE BARREIRO afirma que el bien jurídico protegido en el delito de allanamiento de morada es la intimidad en tanto emanación de la libertad personal al entender que la protección penal de la morada alude a una especial relación de la persona-ambiente en la medida en que ésta aparece reflejada cierta esfera espacial tendente a preservar el carácter íntimo, doméstico o cuando menos privado de determinados comportamientos subjetivos. Por ello concluye que *[e]l derecho a la intimidad alude a una serie de perfiles de la vida privada del ciudadano como el de la protección de la inviolabilidad del domicilio, que se trata de tutelar en el delito de allanamiento de morada.* JORGE BARREIRO, 1987: 27-29.

[93] Algunos autores se refieren al bien jurídico protegido en los artículos 202 a 204 como la intimidad domiciliaria, posición, además, a la que el Código penal de 1995 ha dado respaldo legal. Al respecto cabe señalar, como muy bien indica MORALES PRATS, la vinculación de la tutela domiciliaria al bien jurídico intimidad no contradice en última instancia los planteamientos tradicionales de un sector de la doctrina (SUÁREZ MONTES, MUÑOZ CONDE, GARCÍA VITORIA y QUINTANO) centrados en la delimitación del objeto jurídico de protección en el concepto de morada. En la mayoría de las definiciones doctrinales que se han acuñado sobre la morada, subyace la mencionada vinculación entre las facultades de exclusión de terceros (referidas a un espacio cerrado) y el bien jurídico intimidad, en la medida que aquélla se proyecta a espacios cerrados en el que se desarrollan actividades relativas a la vida privada o funciones domésticas. El domicilio o morada delimita una parcela del bien jurídico intimidad, en cuanto que soporte fáctico-espacial en el que localizan múltiples manifestaciones de la *privacy* de la persona. MORALES PRATS, 2010: 510. BORJA JIMÉNEZ, 1997: 278. MORALES PRATS, 2010: 509. MORALES PRATS, 1996: 242, 279-280. CASTIÑEIRA PALOU, 2010: 154.. GÓMEZ PAVÓN, 1989: 49-50. Defienden igualmente la intimidad como bien jurídico protegido QUERALT JIMÉNEZ, 2010: 283-284. RODRÍGUEZ PADRÓN, 1998: 101.

Planteada en estos términos, el paraguas interpretativo del interés jurídico protegido implica ceñir la tutela penal a todos aquellos accesos que tienen lugar únicamente en relación con sistema cuyo contenido son datos pertenecientes a esta esfera íntima. Lo anterior conduce a excluir la protección de multitud de accesos en los que el contenido del sistema no cumple el perfil indicado, algo que sin lugar a dudas no me parece el fin querido por la norma. El acceso ilícito no se proyecta de forma directa y exclusiva sobre la intimidad personal o familiar, sino sobre todo un conjunto de bienes jurídicos que pueden verse afectados[94].

2. NOCIÓN FÍSICO-ESPACIAL DE DOMICILIO

El segundo motivo por el cual debe descartarse que el domicilio informático sea el bien jurídico protegido en el delito de acceso ilícito tiene su fundamento en la propia configuración constitucional del concepto de domicilio, en relación con el cual habrá que distinguir:

> **a) Domicilio de persona física:** éste es concebido como el espacio físico en el cual el sujeto ejerce su libertad más íntima y desarrolla los actos de su vida privada sin estar sujeto necesariamente a los usos y convenciones sociales[95]. Así pues, el objeto específico de protección en este derecho fundamental es tanto el espacio físico en sí mismo como también lo que en él hay de emanación de la persona que lo habita[96].

---

[94] A favor, SÁNCHEZ DOMINGO, 2012: 33.

[95] Sentencias del Tribunal Constitucional 22/1984, 94/1999, 171/1999, 119/2001 y 10/2002.

[96] Sobre inviolabilidad del domicilio de la persona física véase bibliografía española citada en el Capítulo VI.

b) Domicilio de persona jurídica: el concepto de domicilio viene determinado en este caso por aquellos lugares utilizados por sus representantes para desarrollar sus actividades internas, bien porque en ellos se ejerce la habitual dirección y administración de la sociedad, o bien porque sirve de custodia de documentos u otros soportes de la vida diaria de la sociedad o de su establecimiento[97].

Ahondando en esta idea, la inviolabilidad del domicilio se construye de forma inescindible sobre la conexión de la persona con el ambiente en el que ésta desarrolla su vida privada[98], pudiéndose distinguir dos facetas:

a) Libertad domiciliaria: expresa la idea de prolongación espacial de los ocupantes de la morada o del contexto espacial profesional. Se significa así un contexto en el que es posible el desarrollo autónomo e incondicionado de las formas más elementales de exteriorización de la libertad humana[99], y se garantizan las condiciones fácticas idóneas para la libre realización de comportamientos individuales o familiares en espacios delimitados.

---

[97] Como es sabido, una de las cuestiones más debatidas al amparo de la vigencia del Código penal anterior era su aplicación a las entradas indebidas en el domicilio de las personas jurídicas, ello en tanto en cuanto la STC 137/1985, de 17 de octubre había admitido la titularidad por parte de éstas del derecho a la inviolabilidad del domicilio del artículo 18.2 de la Constitución como un derecho independiente cuando se cumplieran dos condiciones. En este sentido, el artículo 203 del Código penal de 1995 del domicilio social o fiscal despejó las dudas existentes al respecto incriminando la entrada 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. No obstante, el artículo 203 presenta ciertas diferencias en relación con el artículo 202, de las cuales por lo que aquí me interesa resaltar hay que destacar la ausencia de la modalidad pasiva de entrada indebida. En la medida en que se ve protegido tanto en domicilio de las personas físicas como de las jurídicas no obstaría en este caso la afirmación de que es posible cometer. MUÑOZ CONDE, 2010: 290-291.

[98] SUÁREZ MONTES, 1968: 6-8. SANZ MORÁN, 2006: 23.

[99] MORALES PRATS, 2010: 511.

b) Inviolabilidad domiciliaria: se identifica con el *ius prohibendi* en tanto que instrumento jurídico adecuado para preservar la intimidad[100].

En el acceso ilícito el objeto material inmediatamente atacado no es un lugar que por su propia naturaleza presuponga una esfera espacial efectivamente tomada por el sujeto para el desarrollo de los actos de la vida privada[101], sino un mero instrumento de almacenamiento de datos relativos a ésta[102]. El sistema informático tampoco conforma una proyección espacial que garantice el libre desarrollo de la personalidad y, además, permita al individuo organizar sus facultades de exclusión y admisión[103].

En consecuencia, ni la proyección espacial de la personalidad ni vinculación directa del domicilio al desarrollo autónomo de la libertad individual anunciadas pueden predicarse del acceso ilícito poe dos motivos:

a) Porque éste se encuentra vinculado a derechos de diversa índole que no hallan una proyección directa sobre la base del libre desarrollo de la personalidad en un espacio determinado.

b) Porque la introducción física que conformaría la injerencia en el derecho a la inviolabilidad del domicilio no puede producirse en el acceso ilícito a un sistema informático[104], en el cual, además, no es posible la introducción física de la persona

---

[100] MORALES PRATS, 2010: 511.

[101] En cambio, se entiende la intimidad domiciliaria como prolongación espacial de la voluntad del morador constituye el soporte fáctico en el cual la persona ostenta un dominio del contexto de la acción, consistente en facultades de exclusión de terceros, enderezadas a garantizar unas condiciones adecuadas para el libre desarrollo de la personalidad en la privacy doméstica individual o familiar. BORJA JIMÉNEZ, 1997: 278. MORALES PRATS, 2010: 509. MORALES PRATS, 1996: 242, 279-280. CASTIÑEIRA PALOU, 2010: 154. GÓMEZ PAVÓN, 1989: 49-50. Defienden igualmente la intimidad como bien jurídico protegido QUERALT JIMÉNEZ, 2010: 283-284. RODRÍGUEZ PADRÓN, 1998: 101.

[102] BORJA JIMÉNEZ, 1997: 271.

[103] GALÁN MUÑOZ, 2009: 95-96.

[104] MARANI, 2007: 311.

y en el cual la condición ineludible para la realización del tipo es la vulneración de las medidas de seguridad[105].

En Italia se utiliza como argumento por la doctrina el hecho de que el sistema informático no puede ser asimilado a los lugares privados expresamente mencionados en el artículo 614 del Código penal italiano (habitación, lugares de privada morada y sus pertenencias), en cuanto lugares de protección espacial de la persona[106], pero no debe olvidarse que en España existe un reconocimiento del domicilio de las personas jurídicas, debiéndose señalar la mayor amplitud del objeto protegido en el acceso ilícito, siendo que en nuestro ordenamiento jurídico no existe problema alguno desde esta perspectiva para vincular el domicilio informático a la utilización del sistema informático en el ámbito industrial y comercial, así como en el sector público[107].

3. UBICACIÓN SISTEMÁTICA

A ello hay que añadir que si en la mente del legislador español hubiera estado proteger el sistema como manifestación del domicilio debería haber atendido a la propia ubicación sistemática de los delitos contra la inviolabilidad del domicilio informático, situados en el Capítulo II del mismo Título dedicado a la intimidad.

---

[105] CANNATA, 2006: 524. PECORELLA, 2006: 5980.

[106] PECORELLA, 2006: 316.

[107] CANNATA, 2006: 524.

IV. INTEGRIDAD, DISPONIBILIDAD Y CONFIDENCIALIDAD DE LOS DATOS, REDES Y SISTEMAS INFORMÁTICOS

A) CONCEPTO, NATURALEZA Y CONTENIDO DE ESTAS TRES FACULTADES COMO BIEN JURÍDICO PROTEGIDO

Últimamente va cobrando fuerza la tesis de que es la integridad, la disponibilidad o la confidencialidad del sistema el bien jurídico protegido en el delito de acceso ilícito a un sistema informático. Esta postura tiene su fundamento en **el Convenio** sobre Ciberdelincuencia de Budapest de 23 de noviembre de 2001, que hace alusión (en cierta medida indirecta) a estas tres características del sistema, de las redes y de los datos como un nuevo bien jurídico necesitado de tutela penal en el Preámbulo y que **recoge el delito de acceso ilícito entre las *Infracciones contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos*** (artículo 2 del Título 1 de la Sección 1 del Capítulo II)[108].

Además, la integridad, la disponibilidad y la confidencialidad de los sistemas, las redes y los datos ha sido también punto de referencia para la Unión Europea a la hora de definir el concepto de seguridad informática en la Comunicación de la Comisión Europea titulada *Seguridad de las redes y la información: Propuesta para un enfoque político europeo*, que será objeto de análisis en el siguiente epígrafe[109].

---

[108] *Convencidos de que 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.* Preámbulo del Convenio sobre Ciberdelincuencia de Budapest de 23 de noviembre de 2001.

[109] La Comunicación de la Comisión de la Unión Europea titulada *Seguridad de las redes y la información: Propuesta para un enfoque político europeo*, define segurodad informática como la *capacidad de las redes o de los sistemas de información para resistir, con un determinado nivel de confianza, todos los accidentes o acciones malintencionadas que pongan en peligro la disponibilidad, autenticidad, integridad y confidencialidad de los datos almacenados o transmitidos y de los correspondientes servicios que dichas redes ofrecen o hacen accesibles.* Un análisis de esta definición de seguridad informática viene recogida en el siguiente epígrafe de esta sección del capítulo.

En el ámbito comparado (especialmente en Alemania) se ha considerado generalmente como bien jurídico del delito de acceso ilícito a un sistema informático alguna de estas facultades de los sistemas de forma independiente. Así pues, algunos autores han defendido que es la integridad del sistema el objeto jurídico tutelado en el delito[110], otros han entendido que lo es la disponibilidad[111] y, finalmente, unos pocos han interpretado que es la confidencialidad[112] del sistema el interés objeto de tutela. En España, en cambio, RUEDA MARTÍN, la única autora que se ha decantado por esta postura, parece resaltar el carácter pluriofensivo del delito al afirmar que los tres intereses se ven afectados por la conducta típica[113], pero los presenta más bien como un único bien jurídico tricéfalo[114].

---

[110] En Italia, de hecho, existe un fundamento jurídico-legal de esta opinión en la circunstancia agravante prevista en el párrafo 2º del apartado 3 del artículo 615 *ter*, que incrementa la pena por razón del carácter público o militar del sistema informático agredido. ALTENHAIN y WIETZ, 2013: 1588 párrafo 1. CANNATA, 2006: 526. BT-Drucks 16/3656, 2006: 7-9. GRÖSELING y HÖFINGER, 2007: 551. MANTOVANI, 1994: 12, 19. MARANI, 2007: 385. MERLI, 1993: 117, 126. NUNZIATA, 1998: 715. PECORELLA, 2006: 321. PICOTTI, 2004: 76. SIEBER, 2012: C 43.

[111] BOSCH, 2014: 1275 párrafo 1. FISCHER, 2013: 1359 párrafo 2. HOYER, 2012: 2 párrafo 1. GRAF, 2012: 2. JOECKS, 2012: 351 párrafo 1. KARGL, 2013: 1406 párrafo 3. LENCKNER y EISELE, 2010: 2.

[112] ALTENHAIN y WIETZ, 2013: 1588 párrafo 1. DIETRICH, 2009: 27-59. DIETRICH, 2011: 247. ERNST, 2007: 2661. GRAF, 2012: 178 párrafo 2. HEGER, 2014: párrafo 1. HERZOG, 2009: 1-10. HILGENDORF, 2005: 49. HILGENDORF, 2012: 160-161. JESSEN, 1994: 37. KINDHÄUSER, 2013: 744 párrafo 1. LENCKNER y EISELE, 2010: párrafo 1. SCHMITZ, 1995: 478. SCHULZE-HEIMING, 1995: 37. SCHUMANN, 2007: 676.

[113] La autora opina que la afectación de cada uno de estos tres bienes jurídicos se produce con el acceso en la medida en que la integridad se ve afectada por el mero acceso, la confidencialidad puesto que se trata de una persona no autoriza y la disponibilidad a causa del uso por parte de ésta. RUEDA MARTÍN, 2010: 364, 372, 373.

[114] Para RUEDA MARTÍN se trata de bienes jurídicos de carácter colectivo que cumplen las dos funciones que todo bien de estas características tiene encomendadas: una función positiva, permitir que otros bienes jurídicos cumplan su función, y otra negativa, evitar de riesgos para otros bienes jurídicos. RUEDA MARTÍN, 2010: 364, 372, 373.

Explicadas cada una de las distintas posturas existentes al respecto, es necesario en este momento ahondar un poco más en el **contenido** de cada una de estas tres características:

1. INTEGRIDAD DEL SISTEMA

La primera de las características enunciadas es la integridad del sistema. A este efecto, el Convenio sobre Ciberdelincuencia de Budapest de 23 de noviembre de 2001 recoge ciertas acciones que califica como directamente lesivas de la integridad de los datos (artículo 4[115]) o del sistema (artículo 5[116]). La integridad aparece supeditada en el Convenio a la producción de un **perjuicio** para el sujeto pasivo, ya sea desde una perspectiva negativa, en tanto alteración o supresión del contenido del sistema (artículo 4)[117], ya sea positiva, en el sentido de mera obstaculización de su funcionamiento del mismo (artículo 5)[118]. Por el contrario, en la literatura comparada la integridad ha sido vinculada a los propios elementos del sistema y a la protección dispuesta sobre éstos, sin requerir ninguna de las condiciones mencionadas (alteración u obstaculización)[119].

---

[115] *Article 4 – Data interference.*
1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the damaging, deletion, deterioration, alteration or suppression of computer data without right.
2 A Party may reserve the right to require that the conduct described in paragraph 1 result in serious harm.

[116] *Article 5 – System interference.*
Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the serious hindering without right of the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data.

[117] COUNCIL OF EUROPE, 2001: 17 párrafos 60-61.

[118] COUNCIL OF EUROPE, 2001: 19 párrafos 65-66.

[119] En Alemania, la integridad se vincula a la propia protección del sistema a través de las medidas de seguridad. En España, la única definición sobre integridad del sistema la aporta RUEDA MARTÍN, que alude a la utilización del sistema con las pertinentes modificaciones del contenido por parte de la o las personas autorizadas. ALTENHAIN y WIETZ, 2013: 1588 párrafo 1. CANNATA, 2006: 526. GRÖSELING y HÖFINGER, 2007: 551. MANTOVANI, 1994: 19. MARANI, 2007: 385. MERLI, 1993: 117, 126. NUNZIATA, 1998: 715. PECORELLA, 2006: 321. PICOTTI, 2004: 76. RUEDA MARTÍN, 2010: 373. SIEBER, 2012: C 43.

2. DISPONIBILIDAD

La segunda de las características a las que se ha hecho referencia es la disponibilidad del sistema. A pesar de que, como se ha indicado, el Convenio hace referencia a ella en la rúbrica del Título 1, ni el Convenio ni el Informe explicativo proporcionan una definición explícita de lo que debe entenderse como tal[120]. En consecuencia, será necesario acudir a la doctrina comparada para ofrecer una noción de este término. En general, ésta establece una relación directa entre dicho concepto, —al que se hace referencia también como poder de disposición—, y la propia **utilización** del sistema informático[121] o, también, la **accesibilidad** a los datos contenidos en él[122].

---

[120] No obstante, el Convenio se refiere indirectamente a la disponibilidad en el artículo 4 cuando señala que la supresión de los datos afecta también a su disponibilidad, pareciendo concebirse como sinónimo de accesibilidad a los datos. Así, afirma que *[p]or supresión de datos informáticos se entiende cualquier acción que impida o ponga fin a la disponibilidad de los datos para la persona que tiene acceso al ordenador o al soporte de datos en que fueron almacenados*. COUNCIL OF EUROPE, 2001: 17 párrafo 61.

[121] En este sentido, RUEDA MARTIN hace referencia al control sobre la utilización de un determinado sistema por parte de la o las personas autorizadas. RUEDA MARTÍN, 2010: 373-374.

[122] Un sector acreditado de la doctrina alemana considera que el bien jurídico protegido es el poder de disposición del propietario sobre los datos informáticos en relación con los que éste ha dispuesto medios de protección encaminados a impedir su acceso (no se debe perder de vista que el objeto material del delito en este país son los datos sobre los cuales se ha dispuesto algún tipo de protección), siendo que la conducta supone un claro atentado en contra del interés del propietario que ha protegido a los datos contra su acceso no autorizado. En este sentido, para la doctrina alemana son susceptibles de ser diferenciadas dos titularidades: la titularidad sobre los datos y la titularidad sobre el dispositivo de almacenamiento. Ello permite atribuir el poder de autorización del acceso a los datos a quien realizó el acto creador de los mismos (*Skripturakt*), pudiendo éste quedarse la autoridad sobre los mismos o transferir el poder de acceso a otro, siendo que el propietario del dispositivo podrá considerarse como no autorizado a los efectos de la comisión del delito si accede a ellos (*negatives Sonderdelikt*). BOSCH, 2014: 1275 párrafo 1, 1279 párrafo 11. FISCHER, 2013: 1359 párrafo 2. HILGENDORF, 1996: 892. HILGENDORF, 2005: 512. HOYER, 2012: 2 párrafo 1. GRAF, 2012: 184 párrafo 20. JOECKS, 2012: 351 párrafo 1. KARGL, 2013: 1406 párrafo 3. LENCKNER y EISELE, 2010: 2. SCHREIBAUER y HESSEL, 2007: 616.

3. CONFIDENCIALIDAD

La tercera y última de las facultades que el Convenio atribuye al titular del sistema sobre éste es su confidencialidad, que dicha norma no define. La doctrina nuevamente entiende que confidencialidad implica la **restricción de la esfera de utilización y acceso** al sistema y a los datos informáticos en él contenidos a un grupo reducido de personas[123]. Mientras que a primera vista este derecho parece poder predicarse únicamente del propio contenido del sistema informático[124], también es posible enlazarlo con el propio sistema informático, tal y como realiza RUEDA MARTÍN, quien concreta este concepto en la utilización exclusiva por personas autorizadas[125].

---

[123] Así planteado, el concepto de confidencialidad se asemeja muchísimo, aunque no resulta plenamente equivalente, al de privacidad, tal y como éste ha sido configurado en apartados anteriores de éste capítulo. Recuérdese que mientras la intimidad venía a integrarse por aquellas manifestaciones de la personalidad individual o familiar cuyo conocimiento o desarrollo quedan reservados por su titular o sobre las que ejerce alguna forma de control cuando se ven implicados terceros, entendiendo por tales tanto los particulares como los poderes públicos. La privacidad iba referida al conjunto de facetas vinculadas a la personalidad que pueden ser identificadas como manifestaciones de la vida privada. En este sentido, privacidad implica restricción al conocimiento de terceros, siendo la diferencia más patente predicable de ésta en relación con la confidencialidad el ámbito al que ésta se extiende. Así pues, mientras que la privacidad tendría como objeto el ámbito personal del sujeto, la confidencialidad no tendría por qué ir vinculada a la vida privada, pudiendo ser extendida, como se verá en la siguiente nota, a cualquier tipo de contenido que el titular haya querido restringir del acceso de terceros. Véase II. A) 3. b) 2. de la anterior Sección.

[124] En la interpretación de la § 202a, algunos autores alemanes establecen una clara distinción entre la propiedad del sistema, del medio de almacenamiento o del dispositivo de datos y los distintos datos informáticos contenidos en éste. A tal efecto, teniendo en cuenta que dichos datos pueden ser de diferente naturaleza, proponen centrar el bien jurídico en el derecho formal a la confidencialidad sobre los datos, entendido éste como derecho a la restricción o limitación del acceso al contenido intelectual sobre datos que son trasmitidos o almacenados, siempre y cuando tales datos se hallen protegidos contra el acceso no autorizado. ALTENHAIN y WIETZ, 2013: 1588 párrafo 1. DIETRICH, 2009: 27-59. DIETRICH, 2011: 247. ERNST, 2007: 2661. GRAF, 2012: 178 párrafo 2. HEGER, 2014: párrafo 1. HERZOG, 2009: 1-10. HILGENDORF, 2005: 49. HILGENDORF, 2012: 160-161. JESSEN, 1994: 37. KINDHÄUSER, 2013: 744 párrafo 1. LENCKNER y EISELE, 2010: párrafo 1. SCHMITZ, 1995: 478. SCHULZE-HEIMING, 1995: 37. SCHUMANN, 2007: 676.

[125] RUEDA MARTÍN, 2010: 373.

B) VALORACIÓN PERSONAL

Antes de emitir cualquier juicio personal acerca de la integridad, disponibilidad y confidencialidad como bien jurídico en el delito de acceso ilícito, creo que es necesario especificar cuáles serán las facultades concretas que serán objeto de valoración crítica. Pues bien, aunque el Convenio pone en relación tales valores con tres objetos distintos: los sistemas, las redes y los datos, debe descartarse de entrada cualquier vinculación entre el acceso ilícito y la integridad, disponibilidad y confidencialidad de los datos y la de las redes, pues, como se verá, la protección se extiende únicamente al sistema y no a los datos, ya sea almacenados[126], ya sea en proceso de transmisión[127], y, a tal efecto, es preciso que el bien jurídico tenga algún género de proyección sobre el objeto material del delito[128].

Dicho lo anterior, la consideración de estos tres aspectos o si quiera de alguno de ellos como integrantes de un mismo bien jurídico no resulta, en mi opinión, acorde con la pretensión de tutela del delito de acceso ilícito a un sistema informático.

---

[126] Como se verá en el correspondiente capítulo, el objeto material del delito es el sistema y no los datos. Véase Capítulo V.

[127] La afectación de los datos cuando éstos se encuentran en procesos se transmisión se protege a través de lo que se conocen como conductas de interceptación de las comunicaciones. Así, es el término interceptación el que está relacionado con las comunicaciones o transmisiones de datos así como con las radiaciones electromagnéticas que, dentro de éstas, pueden servir para descubrir tales datos. Se refiere, pues, a escuchar, monitorear o vigilar el contenido de las comunicaciones, a adquirir los contenidos de datos de dichas comunicaciones o a la grabación de la mismas. Se trata, en definitiva, de cualquier forma de transferencia electrónica de datos, ya sea por teléfono, fax, correo electrónico o transferencia de archivos, hecho éste último que incluye la interceptación de datos que están siendo enviados dentro de la red electrónica que integra el propio sistema informático, como, por ejemplo, desde el ordenador a la impresora. Esta conducta, cuya finalidad específica atiende a proteger el derecho a la privacidad de las comunicaciones de datos, aparece castigada en el apartado 2 del artículo 197 *bis* de nuestro Código penal y en el segundo inciso del apartado 1 del artículo 197. Véanse respecto de éste último FERNÁNDEZ TERUELO, 2007: 124. ORTS BERENGUER y ROIG TORRES, 2001: 25. ROMEO CASABONA, 2004a: 88, 95.

[128] MORALES PRATS, 2011b: 821.

Por una parte, aunque el Convenio los recoge conjuntamente, lo cierto es que no creo que estuviera en la *mens legislatoris* que estos tres intereses, conjuntamente, fueran el bien jurídico protegido en todos y cada uno de los comportamientos cuya incriminación se propone en el Título 1 de la Sección I del Capítulo II del Convenio sobre Cibercriminalidad de Budapest de 23 de noviembre de 2001[129], con independencia de que, en cierta medida, ello pueda deducirse implícitamente de varios de los apartados del Informe explicativo del mismo[130]. Esta posición resulta, en mi opinión, excesivamente amplia, sobre todo cuando en el Título I del Convenio se prevén un total de cinco conductas totalmente heterogéneas (el acceso ilícito, objeto del presente estudio, la interceptación ilícita, los atentados contra la integridad de los datos, y el abuso de equipos e instrumentos técnicos).

Por lo que se refiere a su concepción disociada, será necesario analizar cada uno de estas tres características en relación con el sistema informático:

> **a) Integridad:** en primer lugar, la integridad no se ve afectada por el delito ya que no se produce ningún perjuicio para el sujeto pasivo, puesto que el delito exige la mera superación de las medidas de la seguridad, es decir, su desactivación, no su menoscabo.
>
> **b) Disponibilidad:** en segundo lugar, la accesibilidad al contenido del sistema no se ve tampoco afectada en el acceso ilícito, debido a que la acción de acceder no tiene por qué impedir la utilización del sistema informático por el titular.

---

[129] Efectivamente, junto al acceso ilícito se propone la incriminación de la interceptación ilícita (artículo 3), de los ataques a la integridad de los datos (artículo 4), de los ataques a la integridad del sistema (artículo 5) y del abuso de dispositivos (artículo 6). Ello no quiere decir que, efectivamente, sean estos tres intereses los protegidos en cada uno de los tipos propuestos, tal y como afirma RUEDA MARTÍN.

[130] COUNCIL OF EUROPE, 2001: 13 párrafo 43-44, 16-17 párrafo 61, 20 párrafo 71.

c) Confidencialidad: en tercer y último lugar, la confidencialidad se encuentra vinculada estrechamente al contenido del sistema informático, la información, y no a éste en cuanto a tal, significando concretamente su circunscripción a un grupo reducido y delimitado de personas, sea por la naturaleza de la información cuanto por la voluntad del titular de la misma[131].

En consecuencia, creo que la realización de la conducta de acceso ilícito no afecta a ninguno de los intereses enunciados, tanto si se entienden de forma conjunta como facultades integrantes de un mismo derecho como si se conciben de forma separada como tres intereses distintos.

[131] ROMEO CASABONA, 1988: 450.

V. SEGURIDAD INFORMÁTICA

Otra de las propuestas que se ha realizado en torno al bien jurídico protegido del delito de acceso ilícito ha sido la relativa a la seguridad informática. Bajo la expresión seguridad informática se ha hecho referencia a todo un conjunto de realidades que tienen como nota común la descripción de una situación de confianza y ausencia de riesgo o lesión para otros bienes jurídicos en el uso de los sistemas informáticos y de las redes telemáticas[132]. Señala a este respecto CARRASCO ANDRINO que la seguridad informática se ha convertido en un valor de primer orden en la nueva sociedad de la información y el conocimiento, al incidir sobre todas aquellas actividades que hoy en día se sustentan sobre ellos[133].

No obstante, se trata de un concepto cuyo contenido no ha sido todavía desarrollado por la doctrina española, hecho que ha conducido a algunos autores a afirmar que carece de autonomía suficiente para sustentar sobre él la tutela penal[134]. Aún así, son cada vez más los autores que proclaman que la seguridad informática constituye un nuevo bien jurídico penal, siendo diversos los enfoques que, en cuanto a contenido, se le ha ofrecido. Véanse cuáles son:

---

[132] Esta idea aparece implícita en la Decisión Marco al indicar en su Considerando (3) la necesidad de un planteamiento global en materia de seguridad de las redes y de la información. La Comisión Europea también adopta como cimiento de la seguridad informática la confianza, al definirla como *capacidad de las redes o de los sistemas de información para resistir, con un determinado nivel de confianza…* COUNCIL OF EUROPE, 2012: 1 y ss.

[133] CARRASCO ANDRINO, 2010b: 250.

[134] Explica RUEDA MARTÍN que la seguridad informática no ostenta un substrato homogéneo, unitario y autónomo en la medida en que no existe una seguridad en sí misma si no es puesta en relación con otros bienes jurídicos. GONZÁLEZ RUS, 2007: 21. RUEDA MARTÍN, 2010: 364.

A) SEGURIDAD COMO EXPRESIÓN DE LA INTEGRIDAD, DISPONIBILIDAD Y CONFIDENCIALIDAD

En el ámbito supranacional es posible hallar una definición de seguridad informática en la Comunicación de la Comisión de la Unión Europea titulada *Seguridad de las redes y la información: Propuesta para un enfoque político europeo*, que la conceptúa como la *capacidad de las redes o de los sistemas de información para resistir, con un determinado nivel de confianza, todos los accidentes o acciones malintencionadas que pongan en peligro la disponibilidad, autenticidad, integridad y confidencialidad de los datos almacenados o transmitidos y de los correspondientes servicios que dichas redes ofrecen o hacen accesibles*[135].

De esta definición se desprenden dos tipologías diferentes de seguridad: aquella que hace referencia a los datos almacenados en los sistemas de información y aquella que engloba a los datos que son transmitidos a través de las redes de información[136].

---

[135] EUROPEAN UNION COMMISSION, 2001: 1 y ss.

[136] Esta es la opción adoptada por MORALES PRATS, quien defiende que es la seguridad de la nueva sociedad de la información concretada en la seguridad de los sistemas informáticos y de las redes el bien jurídico protegido en el delito. Un interés que el autor califica de primer orden en tanto que tiene como finalidad proteger a éstos al efecto de garantizar la confianza y la certidumbre en la autenticidad e integridad de la información que se contiene en los mismos, sobre todo, a la vista de los ataques protagonizados por grupos terroristas o grupos de criminalidad organizada. Por tanto, subyace en el nuevo precepto la idea de reforzar los sistemas básicos de información. La apuesta es, por tanto, de acuerdo con CARRASCO ANDRINO por la seguridad en el tráfico informático y por proteger la integridad y certeza en los datos y programas informáticos. CARRASCO ANDRINO, 2010b: 346. MORALES PRATS, 2011b: 821. MORALES PRATS, 2011a: 482.

B) SEGURIDAD DE LA INFORMACIÓN

ANARTE BORRALLO y DOVAL PAIS defienden que el interés protegido en este caso sería la seguridad de la información que los sistemas informáticos contienen —no la de los sistemas informáticos en sí mismos considerados—[137]. Con respecto a tal objeto, el delito de acceso ilícito se comportaría como una figura de lesión en relación con la redacción de 2010, ya que dichos autores consideran que, en tanto la consumación viene determinada por el acceso o la permanencia, estas conductas suponen evidentemente la vulneración de la seguridad y la intangibilidad de los sistemas informáticos[138] y de peligro abstracto para la intimidad a partir de la redacción de 2015[139]. En consonancia con ello, lo relevante a la hora de acotar la delimitación del ámbito de lo punible no serían cualesquiera medidas de seguridad, sino solo las que garantizan esta seguridad de la información[140].

MATELLANES RODRÍGUEZ se pronuncia en un sentido similar, al entender que el sistema informático en sí también es un valor en sí mismo que puede estar afectando a un interés supraindividual, la seguridad informática o seguridad en el funcionamiento de los sistemas informáticos o confianza en el funcionamiento de éstos, un interés que considera inmaterial, difícil de aprehender y de definir, pero del cual toda la sociedad tiene constancia de su existencia, esto es, de que hoy constituye un ingrediente indispensable para el normal desarrollo de las relaciones del tráfico y que se tambalea peligrosamente cuando se desvelan y salen a la luz determinados supuestos de intrusismo informático[141].

---

[137] ANARTE BORRALLO y DOVAL PAÍS, 2012: 12-13. También ANARTE BORRALLO y DOVAL PAÍS, 2015: 517.

[138] ANARTE BORRALLO y DOVAL PAÍS, 2012: 12-13.

[139] ANARTE BORRALLO y DOVAL PAÍS, 2015: 517.

[140] ANARTE BORRALLO y DOVAL PAÍS, 2012: 12-13. También ANARTE BORRALLO y DOVAL PAÍS, 2015: 517.

[141] MATELLANES RODRÍGUEZ, 2004: 5.

C) CONCEPCIÓN FORMAL

ROVIRA DEL CANTO, en una parte avanzada de su estudio, considera que el acceso ilícito excede de lo que es el estricto ámbito económico, y reconoce que la conducta supone una evidente puesta en grave y serio peligro o riesgo de los nuevos bienes jurídicos propiamente informáticos y de la información, precisos de protección penal sin necesidad ni de una utilización ilícita de los sistemas informáticos de las empresas víctimas, ni de una posterior producción de un efectivo resultado lesivo o perjudicial en el ámbito patrimonial[142].

De este modo, el autor, haciéndose eco de las distintas propuestas internacionales, apuesta terminantemente por la creación de un nuevo bien jurídico de carácter colectivo y autónomo, la seguridad informática, cuyo fundamento se hallaría en el artículo 9.2 de la Constitución y estaría dotada de una función negativa, la de ejercer de barrera anticipada de posibles quebrantos de efectivos bienes jurídicos individuales ya protegidos por el Derecho penal y, una positiva, la de posibilitar a todo ciudadano el uso de sis derechos y libertades e, incluso, aboga por la introducción *ex novo* de un título en el Código penal dedicado a los delitos contra la seguridad informática o seguridad del tráfico informático[143]. Para él, el acceso ilícito constituiría así el tipo básico, de lesión, sobre el que configurar las distintas modalidades de comportamientos que supondrían un atentado contra dicho bien jurídico[144].

GONZALEZ RUS lo concibe como un bien jurídico colectivo que viene a dar protección anticipada a otros de naturaleza personal, como la intimidad, el honor el patrimonio, la libertad de información, el secreto y la inviolabilidad de las comunicaciones[145].

---

[142] ROVIRA DEL CANTO, 2002: 199, 200, 204.

[143] ROVIRA DEL CANTO, 2002: 199, 200, 204.

[144] ROVIRA DEL CANTO, 2002: 199, 200, 204.

[145] GONZÁLEZ RUS, 2007: 15-16.

En su opinión, su lesión se produciría en cuanto se atenga al uso y funcionamiento correcto de redes y sistemas informáticos con conductas como, por ejemplo, el acceso indebido a un ordenador, incluso si no es para realizar una actividad ilícita ulterior[146].

La posibilidad de prohibir tales comportamientos se fundamenta para él en que generan riesgos para los bienes jurídicos personales a cuya protección mediata sirve la seguridad informática[147]. Se trataría, por tanto, de un bien jurídico colectivo e indisponible, en la medida en que las agresiones a la seguridad informática crean riesgos frente a todos los usuarios y no respecto de un sujeto concreto[148]. La necesidad de crear tal bien jurídico se apoya en dos aspectos:

> a) Por una parte, en que el recurso a la exclusiva protección de bienes personalísimos desconoce la relevancia social que ha adquirido Internet como forma de comunicación interpersonal, con identidad y autonomía propia, de manera que la tutela específica y diferenciada cumpliría una función simbólica positiva, estimulando la conciencia social sobre la necesidad de proteger su seguridad y la gravedad del uso y funcionamiento indebidos de las redes[149].
>
> b) Por otra, en que la intervención penal a través de las figuras dirigidas a la protección de los bienes jurídicos individuales requiere probar la motivación y la intención subjetiva del autor respecto del bien jurídico lesionado de manera efectiva, lo que dificulta la protección, dado que en la mayoría de los casos el ataque a la red o al sistema informático no se dirige contra esos bienes jurídicos[150]. Por

---

[146] GONZÁLEZ RUS, 2007: 15-16.

[147] GONZÁLEZ RUS, 2007: 15-16.

[148] GONZÁLEZ RUS, 2007: 15-16.

[149] GONZÁLEZ RUS, 2007: 15-16.

[150] GONZÁLEZ RUS, 2007: 15-16.

eso, estaría justificada la configuración de la seguridad informática como bien jurídico colectivo autónomo y la anticipación de la tutela al momento del peligro[151].

MIRÓ LLINARES, sin embargo, restringe el núcleo del delito a la protección anticipada de la intimidad y del patrimonio en tanto conducta que se ha considerado potencialmente peligrosa para estos bienes jurídicos[152]. Así, obvia la vertiente individual del bien jurídico y define la seguridad informática como aquella protección anticipada del ámbito donde el individuo desarrolla esferas importantes de privacidad y donde también existen otros bienes jurídicos de contenido patrimonial[153]. Considera, pues, que el mero acceso ya supone un riesgo para la privacidad del sistema y que también integra un acto preparatorio previo a la lesión del bien jurídico patrimonio lo que supone la creación de una fenómeno de anticipada intervención también para este bien jurídico[154].

En igual sentido que MIRÓ LLINARES se pronuncia FERNÁNDEZ TERUELO, si bien con una concepción todavía más restringida del bien jurídico que vincula a la protección del secreto[155]. Este autor afirma que la seguridad informática no debe interpretarse en sentido amplio, sino como manifestación concreta de la intimidad en un sentido genérico, entendida ésta como exclusión de los demás de determinada información o datos propios, al margen de su relevancia[156]. En este sentido, afirma que la llamada seguridad informática afecta a la integridad, confidencialidad y disponibilidad del sistema informático y su tutela va orientada a la protección del núcleo periférico o blando de la intimidad (el mero secreto o deseo de exclusión de los demás del acceso a determinados contenidos

---

151 GONZÁLEZ RUS, 2007: 15-16.

152 MIRÓ LLINARES, 2010: 145 párrafo 1439.

153 MIRÓ LLINARES, 2010: 145 párrafo 1439.

154 MIRÓ LLINARES, 2010: 145 párrafo 1439.

155 FERNÁNDEZ TERUELO, 2011: 198-199.

156 FERNÁNDEZ TERUELO, 2011: 198-199.

ubicados en un ámbito informático propio, al margen de la relevancia o trascendencia de aquello excluido)[157].

D) VALORACIÓN PERSONAL

Esta nueva concepción supondría la afirmación del nacimiento de un nuevo bien jurídico, que castiga la potencialidad peligrosa de la conducta para afectar gravemente a los bienes jurídicos especialmente vulnerables frente a empleos clandestinos de la tecnología informática e Internet. Ahora bien, es necesario analizar el origen de este bien jurídico, su origen, si efectivamente está justificada su creación y, en caso afirmativo, su naturaleza y contenido. A este análisis se dedican las páginas que integran la siguiente Sección del presente estudio.

[157] FERNÁNDEZ TERUELO, 2011: 198-199.

VI. OTROS BIENES JURÍDICOS

Si bien las anteriores son las que ha seguido la doctrina mayoritaria, existen, por supuesto, todo un conjunto de propuestas, generalmente aisladas, que intentan poner de relieve la creación de nuevos intereses dignos de tutela distintos a los analizados hasta el momento. Puesto que algunas de ellas hoy se encuentran superadas y otras no han sido lo suficientemente desarrolladas como para dedicarle un epígrafe independiente, serán simplemente enunciadas en el presente apartado.

Desde una concepción originariamente vinculada a la **delincuencia económica**, hoy superada, se propugnaba como bien jurídico protegido en el delito el patrimonio, con base en la atribución de valor económico a la información[158].

---

[158] Puesto que, como se ha indicado en los Capítulos anteriores, la delincuencia informática nació vinculada a la delincuencia económica, algunos autores consideraron que la protección dispensada por los tipos penales dirigidos a castigar la comisión de estos ilícitos, propugnan limitar la tutela penal únicamente a aquellas conductas que afectaran directamente a la datos de contenido económico. En Alemania algunos autores proyectaron el bien jurídico del delito sobre el propio sistema, o bien atribuyendo un valor económico a la información, o bien defendiendo la limitación de la protección de los datos a aquellos que tuvieran algún genero de valor económico. En España, ROVIRA DEL CANTO en una primera aproximación de la que posteriormente se desvinculará atribuye al acceso ilícito un cariz económico. Admite que si bien en él no se produce un efectivo perjuicio patrimonial para el titular o usuario, el acceso ilícito implica en todo caso una clara puesta en peligro de los intereses económico-patrimoniales de éste, puesto que éstos se hallan contenidos en los programas o en los datos mismos a los que se tiene acceso. Así, el perjuicio no se derivaría en este supuesto de la verificación de un daño material sino como consecuencia del riesgo que ha existido de dañar el contenido del sistema informático, añadiendo a ello el esfuerzo o coste que le ha supuesto al titular el establecimiento de las medidas de seguridad para evitar tales accesos no autorizados. No obstante, el autor entiende que dicho perjuicio debería integrarse como una violación formal no del delito de daños sino de la esfera de la privacidad y del secreto o la integridad del sistema informático afectado. Asimismo, no deja de poner de relieve que en muchos supuestos estas conductas de acceso ilegal aparecen configuradas materialmente como actos preparatorios de comportamientos delictivos informáticos más graves, en donde sí aparecen unos perjuicios considerables, que sucede cuando posteriormente los autores usan su experiencia y los conocimientos adquiridos con sus logros de acceso para cometer o favorecer la comisión por terceros de acciones de espionaje, sabotaje o fraude informáticos. AMORE et al., 2006: 96. BÜHLER, 1987: 452. HAFT, 1987: 9. ROVIRA DEL CANTO, 2002: 70, 196. SIEBER, 1977: 98.

Otros autores han puesto el acento en la propia **actividad** del sistema informático, apuntando a su utilización[159], su funcionamiento[160] o la tranquilidad en el uso del sistema[161]. No ha faltado tampoco quien considerara el **propio sistema** como un valor digno de protección[162].

No conviene soslayar tampoco ciertas corrientes centradas en el **aspecto cibernético** de este fenómeno, que señalan al secreto de las comunicaciones[163], la comunicación pacífica a través de redes telemáticas[164] o a Internet en sí misma considerada[165] como interés de salvaguarda.

---

[159] BERGHELLA y BLAIOTTA, 1995: 2330.

[160] CORCOY BIDASOLO, al analizar la introducción de diversos delitos relacionados con la informática a través de la reforma de 2003, se refiere al surgimiento de un nuevo bien jurídico de naturaleza autónoma: el propio sistema informatizado o la confianza en su buen funcionamiento, un interés de carácter supraindividual cimentado en la idea de que el buen funcionamiento de los sistemas es condición indispensable para el normal desarrollo de las relaciones económicas y personales de nuestros días. No obstante, aunque la autora hace referencia a la aplicación de este bien jurídico tanto a las relaciones económicas como personales, en realidad su perspectiva parte de una visión económica y patrimonialista de la delincuencia informática, pues se refiere a tales conductas como fraudes informáticos, utilizando esta expresión como sinónimo de delitos informáticos y distinguiendo como los elementos comunes de todos ellos los siguientes: a) Conducta fraudulenta: uso indebido o fraudulento de elementos informáticos a través de la introducción o manipulación de datos falsos, b) Instrumento: presencia de los componentes físicos y/o lógicos del sistema informático, c) Finalidad: obtención de un beneficio ilícito, directo o indirecto, no necesariamente patrimonial, d) Resultado: perjuicio, no necesariamente patrimonial, de tercero o de la colectividad. CORCOY BIDASOLO, 2007: 10.

[161] GUTIÉRREZ FRANCÉS, 1996: 1182.

[162] MATELLANES RODRÍGUEZ afirma que el sistema informático como tal también constituye un valor, lo que se justifica en la especial trascendencia que tiene hoy éste para la sociedad, pues todos los aspectos de la interacción social dependen de la informática. No obstante, afirma, no debe confundirse éste, objeto material del delito, con el propio bien jurídico. MATELLANES RODRÍGUEZ, 2004: 4.

[163] ALTENHAIN y WIETZ, 2013: 1588 párrafo 1. DI PUNZIO y NATALINI, 2006: 698. CUOMO y IZZI, 2002: 1018, 1021.

[164] ROMEO CASABONA, 2006b: 187-190.

[165] QUINTERO OLIVARES, 2001: 375.

En realidad, el primer grupo de propuestas de la página anterior tienen, a mi juicio, un fundamento similar, centrado en los posibles peligros que las nuevas tecnologías pueden entrañar a través de la realización de distintas acciones humanas, las cuales pueden generar riesgos tanto de carácter individual como colectivo para los usuarios, ahondando así en una de las características que mejor definen el Derecho penal de la sociedad del riesgo, la tutela del pacífico disfrute de las actividades que rodean los actuales focos de riesgo estabilidad[166]. En consecuencia, tales argumentaciones vienen a desembocar en la misma idea, pues la desconfianza y el uso pacífico y sin cortapisas de la tecnología informática, no constituyen más que caras opuestas de una misma moneda: la seguridad informática, a la que se hará referencia en el apartado siguiente.

Las propuestas encaminadas a aspectos vinculados con las redes de comunicación, deben ser descartadas en relación con el acceso ilícito, pues éstas están directamente relacionadas con las conductas de interceptación, que protegen a aquellas contra las escuchas, el monitoreo o la vigilancia de su contenido, así como la adquisición de los datos de dichas comunicaciones o a la grabación de la mismas[167].

---

[166] Así se entiende de las palabras de MATELLANES RODRÍGUEZ cuando afirma que *podemos afirmar que el hacking sobre los sistemas o equipos informáticos puede estar afectando a un interés supraindividual,* y cuando se refiere a él utiliza como sinónimos las expresiones *seguridad informática o seguridad en el funcionamiento de los sistemas informáticos o confianza en el funcionamiento de éstos.* MATELLANES RODRÍGUEZ, 2008: 66.

[167] Se trata, en definitiva, de cualquier forma de transferencia electrónica de datos, ya sea por teléfono, fax, correo electrónico o transferencia de archivos, hecho éste último que incluye la interceptación de datos que están siendo enviados dentro de la red electrónica que integra el propio sistema informático, como, por ejemplo, desde el ordenador a la impresora. Véase Apartado 3. del Epígrafe II, nota 111.

SECCIÓN 3ª

TOMA DE POSTURA

LA SEGURIDAD INFORMÁTICA COMO BIEN JURÍDICO PROTEGIDO EN EL ARTÍCULO 197.1 *BIS*

VII. TOMA DE POSTURA: LA SEGURIDAD INFORMÁTICA COMO BIEN JURÍDICO PROTEGIDO

En las últimas décadas, el surgimiento de la sociedad del riesgo ha originado un aumento de las demandas sociales de punición para afrontar la potencialidad dañosa que de ésta se deriva. Uno de los motivos de mayor preocupación social se concreta en el elevado riesgo que para los bienes jurídicos con relevancia penal supone a día de hoy la generación de nuevas agresiones a los mismos, fruto, básicamente, del avance tecnológico.

La delincuencia informática constituye, así, uno de los principales exponentes de la sociedad del riesgo, no resultando sorprendente que haya sido el sustrato perfecto para el alumbramiento de nuevos intereses supraindividuales, tan íntimamente vinculados a ella[168]. Como es sabido, lo anterior tiene su reflejo también en el Derecho penal, ámbito en el cual esta inflación se traduce en la ampliación a veces excesiva de los bienes jurídico-penales[169]. Sin embargo, parece emerger cada vez más un interés público que se manifiesta en la idea de que la perturbación de la utilización de las nuevas tecnologías y, muy especialmente, la informática afecta gravemente a la confianza y seguridad de los demás miembros de la sociedad, que se afana en reclamar tutela frente a los ilícitos derivados de la misma[170]. Este designio constituye, en mi opinión, legitimación suficiente para defender la existencia de un nuevo valor social vinculado al hecho informático[171].

---

[168] CUESTA PASTOR, 2002: 92.

[169] SILVA SÁNCHEZ, 2001: 1 y ss, VARGAS PINTO, 2007: 62.

[170] VARGAS PINTO, 2007: 103.

[171] CORCOY BIDASOLO, 1999: 218.

A) JUSTIFICACIÓN DE LA INTERVENCIÓN PENAL

La extrema relevancia que las nuevas tecnologías están adquiriendo en nuestra sociedad actual para el desarrollo individual, económico y social de los ciudadanos ha conducido, por tanto, al surgimiento de un nuevo interés vinculado a los mismas, un nuevo valor susceptible, merecedor y necesitado de tutela penal con plena identidad y autonomía propia: la seguridad informática[172].

La creación del bien jurídico seguridad informática se justifica, de este modo, en la idea de que la única manera de defender el interés personal de los propietarios de los sistemas es a través de la salvaguarda de un bien común: la confianza en la utilización lícita de las nuevas tecnologías[173].

Aunque la protección de este nuevo valor social incumbe a todo el ordenamiento jurídico, al Derecho penal le corresponderá su salvaguarda frente a las formas más graves de agresión, cuando las sanciones de otros sectores del ordenamiento jurídico no sean suficientes[174].

---

[172] La idea de un bien jurídico sustantivo vinculado al hecho informático no va a suponer, como es obvio, que cualquier conducta delictiva relacionada con las nuevas tecnologías deba necesariamente lesionar este bien jurídico y, por tanto, ser ubicada entre los delitos informáticos en su sentido más específico. Muchas de las conductas que sin duda pueden incluirse entre lo que es la delincuencia informática, como categoría criminológica, dañan únicamente bienes jurídicos tradicionales a través de nuevos medios más sofisticados, pero nada más.

[173] La seguridad informática es un bien jurídico protegido de carácter supraindividual y en cuanto tal, como muy bien indica CORCOY BIDASOLO, su función es proteger la seguridad y la confianza de los ciudadanos en el buen funcionamiento y en el nivel de riesgo de las distintas actividades que, por su naturaleza o concreta situación en el entramado social, se consideran más débiles. CORCOY BIDASOLO, 1999: 208.

[174] MAYO CALDERÓN, 2005: 64.

La sanción penal de los ataques a la seguridad informática responde, por consiguiente, a una necesidad no cubierta por el Derecho penal de establecer niveles de protección frente a los cada vez más generalizados ataques a los sistemas informáticos, que son el principal foco de riesgo para la lesión de multitud de bienes jurídicos[175]. Esta idea determina, además, que se utilice la técnica de los delitos de riesgo y se atribuya a dicho valor una naturaleza colectiva[176], pues adquiere su dimensión social en atención a la posibilidad de la multiplicación del riesgo que las conductas vinculadas al hecho informático pueden entrañar[177]. En consecuencia, a través la tutela de este nuevo bien jurídico-penal se pretende garantizar el conjunto de condiciones que, en primer término, posibiliten el uso de las nuevas tecnologías y, en segundo término, salvaguarden los distintos bienes jurídicos que podrían verse imbricados en su ejercicio[178].

En definitiva, creo que, en aras a que los ciudadanos puedan ejercer sus derechos en toda su amplitud, es hora de reconocer que ha nacido un nuevo bien jurídico, un interés con identidad y autonomía propia: la seguridad informática[179], a cuyo estudio y análisis en profundidad se dedicarán las próximas páginas del presente capítulo.

---

[175] Está en lo cierto CARRASCO ANDRINO cuando indica que la necesidad de protección en el ámbito penal se podría fundamentar, por un lado, en su papel de barrera y obstáculo para evitar la lesión de bienes jurídicos individuales, más vulnerables en la nueva sociedad de la información; y por otro en la insuficiencia de los preceptos penales existentes para abarcar tales riesgos. CARRASCO ANDRINO, 2010b: 344.

[176] CUESTA PASTOR, 2002: 222.

[177] CUESTA PASTOR, 2002: 222.

[178] CUESTA PASTOR, 2002: 222.

[179] CUESTA PASTOR, 2002: 222. GONZÁLEZ RUS, 2007: 15-16.

B) ENGARCE CONSTITUCIONAL

Para determinar conforme al principio de ofensividad un bien jurídico de naturaleza colectiva es necesario elaborar un contenido material del mismo y este contenido esencial debe tener raíz en los bienes jurídicos recogidos en la Constitución[180]. Así, el Derecho penal sólo puede salvaguardar bienes jurídicos que o bien estén integrados en la Constitución o bien sea de los denominados implícitos o integrables en la misma[181].

Si bien en la Norma Suprema no aparece ninguna referencia expresa a la seguridad informática, ésta conforma, en mi opinión, un interés jurídico plenamente integrable en la misma, concretamente en su artículo 18.4, el cual reza: *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,* y solo indirectamente en el artículo 9.2 considerado fundamento de aquél por parte de ROVIRA DEL CANTO[182].

A pesar de que dicho apartado se encuentra en sede de la consagración constitucional del derecho a la intimidad, la doctrina considera que en él se recoge una cláusula genérica que no se refiere a los derechos que en él se mencionan y que propugnan los apartados anteriores, sino que las repercusiones de la informática rebasan la mera puesta en peligro o lesión de los mismos, esencialmente vinculados todos ellos a la intimidad[183].

---

[180] CUESTA PASTOR, 2002: 231.

[181] CUESTA PASTOR, 2002: 115. ALVAREZ GARCÍA, 1991: 36.

[182] ROVIRA DEL CANTO, 2002: 199, 200 y 204.

[183] MADRID CONESA, 1984: 59. ROMEO CASABONA, 1988: 29.

Así pues, el engarce de este nuevo interés a la Constitución se produce en relación con ese otro conjunto de derechos a los que ésta hace referencia y que se relacionan con la informática sin constituir expresión más o menos directa de la intimidad o de cualquiera de sus manifestaciones, hecho que vendría expresado en la parte final del texto citado, esto es, en la alusión al *pleno ejercicio de sus derechos*[184].

---

[184] Como es sabido, la configuración de la intimidad como derecho fundamental es controvertida, ya que las opiniones acerca de la autonomía de este derecho han sido divergentes, existiendo serias dudas sobre su delimitación conceptual respecto de los dos derechos que se consagran en el mismo apartado: el honor y la propia imagen y también en relación con los derechos a la inviolabilidad del domicilio y al secreto de las comunicaciones previstos en los apartados 2 y 3 del artículo 18, respectivamente, concebidos en ocasiones como derivaciones de la intimidad.

Lo cierto es que la intimidad es lo que se ha venido a denominar un derecho de derechos, un derecho conforma la base y el fundamento para la protección de la persona en las distintas situaciones que le son propias y que se configura como una realidad jurídica compleja, dinámica y en constante evolución. Estas características –complejidad y dinamismo– se manifiestan en lo siguiente:

Por una parte, la intimidad constituye el telón de fondo de múltiples derechos, los cuales, si bien en tanto derechos autónomos se definen e interpretan sobre la base de indicadores que les son propios, nunca llegan a desvincularse del todo de ésta, que les proporciona criterios generales y comunes para ofrecer cobertura a situaciones que no llegan a encajar dentro de las fronteras de cada uno de ellos en concreto.

Por otra parte, la aparición cada día de nuevas formas de vulnerabilidad de este derecho ha supuesto el desbordamiento del contenido constitucional clásico de la intimidad, obligando a la doctrina y a la jurisprudencia a revisarlo y a actualizarlo al efecto de lograr delimitar nuevamente su alcance y contenido, reformulando los criterios de protección para hacerlos más adecuados y capaces de abarcar las nuevas agresiones que se consideren intolerables a efectos de salvaguardar los aspectos íntimos de la vida de la persona, cuya afección puede resultar no solo de las nuevas facetas de la propia intimidad sino también de situaciones derivadas de los derechos con los que guarda algún tipo de vinculación.

ROVIRA SUEIRO, 1999: 25. GARCÍA GARCÍA, 2003: 183. ALEGRE MARTÍNEZ, 1997: 49. BLASCO GASCÓ, 2007: 60-65. BLASCO GASCÓ, 2008: 14-15. CASTILLA BAREA, 2011: 34. DE VERDA Y BEAMONTE, 2011: 26. HERRERO TEJEDOR, 1998: 167. LÓPEZ DÍAZ, 1996: 28. PARDO FALCÓN, 1992: 166. PASCUAL MEDRANO, 2003: 36, 41. RUIZ MIGUEL, 1995: 76. VIDAL MARTÍNEZ, 1984: 35. O'CALLAGHAN MUÑOZ, 1991: 96. OLIVEROS LAPUERTA, 1980: 21. MARTÍNEZ DE PISÓN CAVERO, 1993: 87. RODRÍGUEZ RUIZ, 1998: 23.

A mi parecer, este apartado de la Constitución debe ser interpretado conforme a la nueva realidad social, que reclama incesante la renovación de su contenido conforme a este nuevo interés que constituyen las nuevas tecnologías, y que se manifiesta en la idea de que la perturbación de la utilización de la informática afecta gravemente a la seguridad de los demás miembros de la sociedad[185].

No creo que, sin embargo, pueda considerarse que el reconocimiento de la seguridad informática como bien jurídico haya sido totalmente desconocido para nuestra Norma Constitucional, cuyo tenor ya auguró en su día la potencialidad dañosa de la informática. En este sentido, la flexibilidad y apertura en su redacción permiten su introducción sin excesivos quebrantos y sin que se produzca una indeseada difuminación de lo penalmente protegible[186].

La Constitución marca el camino de este nuevo interés producto del propio desarrollo del individuo en la sociedad, hoy tecnológica, y que progresivamente ha ido aflorando fruto de la unión del conjunto de intereses individuales que han pasado a suscitar el interés de la comunidad[187] y que le han hecho adquirir una dimensión precisa en la sociedad[188], aunque sin dejar de vislumbrar en él cierta vinculación con el individuo[189]. A estos dos aspectos, el individual y el colectivo, se dedicará el próximo apartado.

---

[185] VARGAS PINTO, 2007: 103.

[186] ALVAREZ GARCÍA, 1991: 36.

[187] Se trata de lo que SCHÜNEMANN refiere como bienes jurídicos supraindividuales de carácter aparente. SCHÜNEMANN, 2002: 185 y ss.

[188] ALVAREZ GARCÍA, 1991: 39. SILVA SÁNCHEZ, 2001: 36-37.

[189] VARGAS PINTO, 2007: 113.

C) NATURALEZA JURÍDICA

Desde la perspectiva anunciada, la seguridad informática se presenta claramente como interés de carácter supraindividual, pero con una clara referencia a otros bienes jurídicos a los que ofrece una tutela de forma mediata[190], hecho que no obsta para afirmar su autonomía. El siguiente paso lo constituirá, por tanto, el análisis más concreto de esta doble naturaleza.

1. EL BIEN JURÍDICO SUPRAINDIVIDUAL INMEDIATAMENTE PROTEGIDO: LA SEGURIDAD INFORMÁTICA

La seguridad informática constituye un nuevo bien jurídico **colectivo** porque, si bien puede afirmarse que existe en ella una combinación de aspectos individuales y colectivos como en todo bien jurídico penal, es la primacía del carácter supraindividual en la ponderación de éstos la que se impone por encima del bien personal de cada sujeto afectado[191].

Todos y cada uno de los miembros de la sociedad comparten el **mismo interés** en lograr el mantenimiento de las condiciones necesarias para garantizar la utilización lícita de las nuevas tecnologías[192]. Se trata, en

---

[190] Como es sabido, la cuestión relativa a la legitimación de los bienes jurídicos supraindividuales es uno de los aspectos más conflictivos de la dogmática actual en dos sentidos. Por una parte, porque cierto sector de la doctrina se ha posicionado críticamente en contra de lo que ha llamado la huida o la expansión del Derecho penal, manifestándose claramente a favor de un Derecho penal de mínimos y de lo que se ha denominado la teoría personalista del bien jurídico, según la cual el bien jurídico supraindividual conduce inexorablemente a la desmaterialización y disolución del concepto de bien jurídico. Por otra parte, pueden hallarse dos vertientes dentro de la propia corriente que acepta la legitimidad de los bienes jurídicos colectivos: aquellos autores que manifiestan la necesaria existencia de un bien jurídico individual de referencia para otorgar legitimación al bien jurídico otorgando así al bien supraindividual un carácter formal, y aquellos que aceptan la existencia de bienes jurídicos de carácter supraindividual dotados de autonomía en cuanto tales. No es materia del presente estudio analizar los distintos posicionamientos en relación con las dos cuestiones anunciadas, si bien ello no obsta a indicar que, a mi juicio, la existencia de bienes jurídicos de carácter supraindividual, siempre y cuando se halle la correcta fundamentación dogmática, es un mal -si así se quiere ver- necesario para culminar las expectativas de la actual sociedad sin sucumbir a los riesgos que ponen en peligro la propia supervivencia colectiva. BUSTOS RAMÍREZ, 1986: 147 y ss.. MAYO CALDERÓN, 2005: 36, 44.

[191] VARGAS PINTO, 2007: 104.

[192] VARGAS PINTO, 2007: 106.

este sentido, de una situación que incumbe no a cada ciudadano por separado sino a la generalidad de los integrantes de la sociedad en su conjunto, pues el respeto a dicho bien jurídico es interés de todos[193]. La **titularidad** del bien jurídico pertenece a todos los miembros de la sociedad conjuntamente considerados[194], con independencia de que la protección de este interés social sirva a todos los ciudadanos para lograr su pleno desarrollo como personas individuales[195].

La seguridad informática es, pues, un bien jurídico supraindividual de **carácter puro**, ello por su contenido, ya que resulta indispensable para garantizar el funcionamiento del sistema teniendo como función la satisfacción de las necesidades sociales[196] y que se encuentra vinculado a la protección de distintos derechos de corte individual y colectivo[197].

La seguridad informática comprende, en consecuencia, el ejercicio de determinadas condiciones de seguridad para el funcionamiento de sistemas y para el goce tranquilo de determinados derechos o bienes individuales[198]. Brinda protección como una barrera previa a todo un conjunto de bienes jurídicos protegidos en otros ilícitos con un mayor contenido de injusto[199]. Así pues, se trata de un bien jurídico de sujeto múltiple del que nadie puede disponer y cuya manifestación colectiva se manifiesta además en la existencia de un interés particular en cada uno de los sujetos implicados[200].

---

193 VARGAS PINTO, 2007: 106.

194 VARGAS PINTO, 2007: 106.

195 CORCOY BIDASOLO, 1999: 204.

196 Es lo que CARBONELL MATEU y SOTO NAVARRO denominan bienes supraindividuales de supervivencia o titularidad colectiva o bienes indivisibles en intereses individuales, esto es, aquellos indispensables para posibilitar las condiciones mínimas de convivencia cuya vulneración ataca la propia existencia de la sociedad BUSTOS RAMÍREZ, 1986: 199-202. CARBONELL MATEU, 1994: 17-29.

197 No se trata, por tanto, de un bien jurídico difuso, ya que la seguridad informática tiene entidad propia en tanto interés a proteger, radicando su razón de ser en el sentido que le otorgan otros bienes jurídicos de naturaleza individual y colectivo. CUESTA PASTOR, 2002: 101.

198 VARGAS PINTO, 2007: 136.

199 MORALES PRATS, 2011b: 819-820.

200 CUESTA PASTOR, 2002: 226.

2. BIENES JURÍDICOS MEDIATAMENTE PROTEGIDOS

Teniendo en cuenta su naturaleza colectiva, el acceso ilícito se presenta como el delito básico contra las amenazas y ataques a la seguridad informática[201], puesto que pretende proteger a los usuarios legítimos de los sistemas informáticos contra las intromisiones que puedan conducir potencialmente a la comisión de ulteriores ilícitos con un mayor contenido de injusto[202]. Tutela, claramente, un bien jurídico de carácter supraindividual con referencia a otros bienes jurídicos, hecho que no obsta, como he dicho, para afirmar su autonomía. Al bien jurídico supraindividual, la seguridad informática, se le dispensará una tutela inmediata, mientras que el resto de intereses serán protegidos en el delito de forma mediata.

Es preciso, por consiguiente, poner en relación la dimensión colectiva de la seguridad informática con los distintos bienes jurídicos individuales que le sirven de fundamento. Aunque otros autores lo han hecho[203], no me parece adecuado ofrecer un catálogo cerrado de todos y cada uno de los bienes jurídicos respecto de los que el acceso ilícito pretende constituir una barrera previa de punición. La razón de lo anterior estriba en el hecho de que el avance constante e ininterrumpido de las nuevas tecnologías incrementa cada día más las posibilidades de ataque a distintos bienes jurídicos. En estos ataques pueden verse afectados tanto intereses con relevancia penal como bienes con relevancia meramente constitucional y que no hayan protección a través de esta rama del Derecho.

---

201 COUNCIL OF EUROPE, 2001: 13 párrafo 44.

202 COUNCIL OF EUROPE, 2001: 15 párrafos 51-52.

203 Cabe recordar que GONZALEZ RUS hace referencia a la intimidad, el honor, el patrimonio, la libertad de información y al secreto y la inviolabilidad de comunicaciones. MIRÓ LLINARES a la intimidad y al patrimonio y FERNÁNDEZ TERUELO únicamente a la intimidad. Por ejemplo, SIEBER, 1992: 77.

En mi opinión, en el delito de acceso ilícito a un sistema informático pueden verse mediatamente afectados los siguientes bienes jurídicos: la intimidad, la propia imagen, el honor, el patrimonio, el orden socioeconómico (y, dentro de éste, la propiedad intelectual, la propiedad industrial y los intereses relativos al mercado y a los consumidores como el secreto de empresa), en ciertos casos también la Administración de Justicia y la Administración pública, el tráfico jurídico (Falsedades), los intereses del Estado (seguridad nacional), la libertad de culto, de conciencia e ideológica y la libertad de información.

Teniendo en cuenta el conjunto de intereses en juego, el elemento que diferencia el delito de acceso ilícito del resto de tipos penales de naturaleza supraindividual se cifra en el hecho de que constituye una anticipación de la tutela penal tanto de bienes jurídicos de naturaleza individual como de intereses de índole colectivo, hecho que supone una importante innovación respecto de la configuración tradicional de este tipo de bienes jurídico-penales, que habitualmente se nutrían únicamente de intereses con naturaleza individual[204].

Sin perjuicio de este especial carácter del bien jurídico protegido, cabe decir que el acceso ilícito no implica la lesión de ninguno de ellos, planteándose habitualmente, en caso de que se llegue a lesionar alguno de estos intereses, un **concurso de delitos ideal medial** en el que el acceso ilícito conformará el medio necesario para cometer el fin delictivo que el sujeto deseaba obtener[205].

---

[204] Sobre el carácter únicamente individual de los bienes mediatamente protegidos véase CUESTA PASTOR, 2002: 241.

[205] MORÓN LERMA considera que el concurso de delitos supone una elevación desproporcionada de la pena. En contra, RODRÍGUEZ MORÓN LERMA, 2002: 69. MATELLANES RODRÍGUEZ, 2004: 6.

D) NÚCLEO ESENCIAL DEL DERECHO: VERTIENTE POSITIVA Y NEGATIVA DEL MISMO

Aunque la seguridad informática sea un derecho que tenga como función secundaria la anticipación de la tutela penal respecto de determinados bienes jurídicos, no se trata de un bien jurídico de los que se ha venido a denominar intermedio o de carácter puramente formal, pues no conforma simplemente una pieza intermedia e instrumental a través de la cual se pretende garantizar la integridad de otros bienes específicos[206]. Ésta constituye un bien jurídico de naturaleza autónoma, pudiendo diferenciarse en su contenido tanto una vertiente positiva como otra negativa, y que integrará el núcleo material del mismo, permitiendo afirmar su autonomía conforme al principio de ofensividad[207].

a) Desde una **perspectiva positiva**, la seguridad informática implica un derecho a poder ejercer el disfrute de la informática como ciudadano libre[208].

b) Desde una **perspectiva negativa**, implica salvaguardar un ámbito de no interferencia en el uso de la informática por parte de los poderes públicos y de los ciudadanos[209].

---

[206] En contra, MATELLANES RODRÍGUEZ, 2008: 67.

[207] CUESTA PASTOR, 2002: 231.

[208] VIVES ANTÓN, 1995: 393.

[209] VIVES ANTÓN, 1995: 392.

E) AFECTACIÓN DE LA SEGURIDAD INFORMÁTICA

Siendo que el acceso ilícito se ha configurado como un delito que atiende a la protección en definitiva de distintos bienes jurídicos, es indudable afirmar que se trata de un fenómeno de criminalización anticipada. A continuación, se hace imprescindible analizar la configuración positiva de esta anticipación de la tutela penal desde la perspectiva del bien jurídico protegido, estableciendo la forma en que el bien jurídico se ve afectado.

Habrá que analizar, pues, si se trata de un tipo de peligro que no precisa lesionar el bien jurídico[210] —tanto si requiere un resultado de peligro (peligro concreto) o se castiga meramente una acción típicamente peligrosa en abstracto sin que se haya puesto en efectivo peligro el bien jurídico[211]—, o si la pretensión de incriminación de la conducta es sancionar ya en un estadio previo a la propia puesta en peligro del bien jurídico, tratándose, en este caso, de un delito obstáculo[212]. Por supuesto, en el ámbito doctrinal no han faltado autores que se hayan pronunciado en cualquiera de los tres sentidos[213].

---

[210] CUESTA PASTOR, 2002: 39.

[211] RODRÍGUEZ MONTAÑÉS, 1994: 14.

[212] MENDOZA BUERGO, 2001: 14.

[213] Consideran que se trata de un delito de **peligro abstracto**: BORRUSO, 1994: 28. DE SANZO et al., 2009: 896, 898. FISCHER, 2013: 1401 párrafo 2. FONDAROLI, 1996: 311. GRAF, 2012: 178 párrafo 3. MATELLANES RODRÍGUEZ, 2008: 66. MIR PUIG, 2002: 301. MERLI, 1993: 126. PECORELLA, 2006: 335. PECORELLA, 2011: 5982. TRENTACAPILLI, 2002: 1283. . De **peligro concreto** MAIORANO, 2010: 1357. . Se decantan por la estructura de **lesión**: CADOPPI et al., 2011: 535-536. CANNATA, 2006: 537. DELPINO, 2003: 584. DESTITO et al., 2007: 82. MANTOVANI, 2011: 543, 544, 546. MARANI, 2007: 622. NUNZIATA, 1998: 715. PARODI y CALICE, 2001: 64. PICA, 1999: 58. RELLA, 2007: 43. VITARELLI, 2011: 399. . En España, consideraban el artículo 197.3 un **delito obstáculo**: FERNÁNDEZ TERUELO, 2011: 198. MATELLANES RODRÍGUEZ, 2008: 68. PUENTE ABA, 2004: 400.

1. ACCESO ILÍCITO COMO DELITO OBSTÁCULO

Como es sabido, los **delitos obstáculo** castigan la llamada premisa idónea, es decir, actos que son necesariamente idóneos para la comisión de un hecho delictivo posterior, que es en última instancia lo que se trata de evitar[214], siendo que, aunque en realidad el bien jurídico no entra en escena hasta un momento posterior, el fundamento de la intervención penal está justificado a los efectos de evitar la comisión de un delito posterior[215]. Si bien es cierto que esta idea podría casar con la conducta de acceso ilícito, son tres los factores que impiden que pueda atribuírsele esta estructura:

> **a) Existencia de bien jurídico:** el bien jurídico inmediatamente afectado en el delito de acceso ilícito es plenamente identificable. Así pues, aunque dicho tipo penal constituye una barrera de punición previa para distintos valores, su comisión ya supone la afectación de un bien jurídico con entidad propia: la seguridad informática[216].
>
> **b) Naturaleza:** el delito de acceso ilícito tiene una naturaleza de delito de riesgo, categoría generalmente excluyente de la figura del delito obstáculo[217].
>
> **c) Posibilidad de lesión del bien mediato:** la mayor parte de los bienes jurídicos que el acceso ilícito salvaguarda de forma indirecta podrán ser no sólo puestos en peligro, sino también lesionados[218].

---

[214] CUESTA PASTOR, 2002: 41.

[215] CUESTA PASTOR, 2002: 47. MATA Y MARTÍN, 1997: 41-45, 49, 56, 82, 85-88.

[216] CUESTA PASTOR, 2002: 317. MATA Y MARTÍN, 1997: 41-45, 49, 56, 82, 85-88. VARGAS PINTO, 2007: 39.

[217] CUESTA PASTOR, 2002: 69.

[218] CUESTA PASTOR, 2002: 69.

2. ACCESO ILÍCITO COMO DELITO DE PELIGRO

Como se ha dicho, si bien la seguridad informática constituirá un bien jurídico independiente, su protección se halla vinculada a la protección de determinados intereses que el acceso tendrá como misión proteger en segunda instancia. Su fundamento será, por tanto, la evitación de la lesión de tales bienes jurídicos[219] con el fin de alcanzar ciertos niveles de funcionalidad y desarrollo de la informática que garanticen al ciudadano el ejercicio de la misma en términos de seguridad y confianza[220], propios de los delitos de riesgo[221]. Desde esta perspectiva habrá que establecer si se trata de un delito de peligro concreto o abstracto.

a) DEROGADO ARTÍCULO 197.3: PELIGRO CONCRETO PARA LA INTIMIDAD

El hoy en día derogado apartado 3 del artículo 197, vigente entre 2010 y 2015, constituía, en mi opinión, un delito de **peligro concreto[222]**, puesto que, tal y como estaba configurada la conducta, el acceso y la permanencia en el sistema producían una situación objetiva de posibilidad de conocimiento/descubrimiento y, por ende, de lesión de la intimidad[223].

---

[219] CUESTA PASTOR, 2002: 55. MATA Y MARTÍN, 1997: 76.

[220] CORCOY BIDASOLO, 1999: 227.

[221] CORCOY BIDASOLO, 1999: 323.

[222] En contra, ANARTE BORRALLO y DOVAL PAÍS entendían que *se adelanta el umbral típico hasta incorporar estadios previos, lo que convierte al precepto en una figura de peligro en relación con la intimidad y los datos personales, que sería abstracto puesto que se presumiría de la ejecución de las acciones seleccionadas (acceso y mantenimiento).* ANARTE BORRALLO y DOVAL PAÍS, 2012: 15.

[223] Podía distinguirse la conducta del sujeto activo (vulneración de medidas de seguridad y acceso) de la situación de peligro producida como consecuencia de aquella (peligro para el contenido íntimo del sistema informático), resultado de aquella. MENDOZA BUERGO, 2001: 24. VARGAS PINTO, 2007: 242.

Esta situación de peligro que se crea con el acceso ilícito se verificaba desde el momento en que se vulneraban las medidas de seguridad y se producía el acceso, siempre y cuando resultara la presencia de elementos que determinaban la existencia del bien jurídico tutelado. De esta forma, si el sistema informático no contenía ningún dato íntimo, no se había producido situación de peligro y, por tanto, la conducta era atípica[224].

b) ARTÍCULO 197.1 *BIS*: DELITO DE PELIGRO ABSTRACTO

i) MODALIDAD DE ACCESO

Mientras que en el artículo 197.3 sólo podía verificarse un peligro en relación con los datos íntimos, conforme a la nueva redacción el acceso inconsentido unido a la vulneración de las medidas de seguridad genera una probabilidad de lesión para los intereses contenidos en el sistema, que puede materializarse en distintos bienes jurídicos[225]. En este caso, a través de la salvaguarda de la seguridad informática se está garantizando la creación de unas condiciones seguras[226] para el ejercicio de derechos de diferente naturaleza[227] . Ésta actúa como una barrera de protección de bienes jurídicos individuales, siendo que mediante la protección del peligro se evita la lesión de tales derechos[228]. Por tal razón, podrá afirmarse que el acceso al sistema puede ser considerada una conducta peligrosa y, en consecuencia, creadora de una situación objetiva de peligro[229].

---

[224] Sobre delitos de peligro concreto MENDOZA BUERGO, 2001: 25.

[225] Sobre delitos de peligro abstracto CUESTA PASTOR, 2002: 70.

[226] ACALE SÁNCHEZ, 2002: 29. RODRÍGUEZ MONTAÑÉS, 1994: 37.

[227] MENDOZA BUERGO, 2001: 241.

[228] CUESTA PASTOR, 2002: 55. CORCOY BIDASOLO, 1999: 326.

[229] Consideran que se trata de una conducta de peligro abstracto aunque entienden que el bien jurídico es la intimidad CASTIÑEIRA PALOU y ESTRADA CUADRAS, 2015: 163. Sobre esta característica en los delitos de peligro véase MENDOZA BUERGO, 2001: 23.

ii) MODALIDAD DE MANTENIMIENTO

También la acción de permanencia no autorizada en el sistema responde claramente a esta estructura de **peligro abstracto**. En este caso, a través de la salvaguarda de la seguridad informática, un bien jurídico-penal de carácter colectivo, se está garantizando la creación de unas condiciones seguras[230] para el ejercicio de derechos de diferente naturaleza[231], pero, a diferencia de lo que ocurre en la acción de acceso, en este caso no existe una aproximación efectiva a ellos[232]. No puede verificarse, por tanto, un resultado de peligro separado de la acción, pues se trata de una mera actividad en que la efectiva producción de una situación de riesgo para el bien jurídico mediato se produce *ex ante*[233].

3. ACCESO ILÍCITO COMO DELITO DE LESIÓN-PELIGRO

El delito de acceso ilícito así concebido gozaría de una doble naturaleza por lo que respecta a la afectación del bien jurídico. Concretamente, se trataría de un delito de los denominados de **lesión-peligro**[234] en el que se distinguiría, por tanto, la lesión de un bien jurídico de carácter colectivo o supraindividual, la seguridad informática, y, en la medida en que éste se configura en relación con bienes individuales, la afectación de estos últimos quedaría limitada a una situación de peligro.

---

[230] ACALE SÁNCHEZ, 2002: 29.

[231] MENDOZA BUERGO, 2001: 241.

[232] MATA Y MARTÍN, 1997: 41-45, 49, 56, 82, 85-88. VARGAS PINTO, 2007: 39.

[233] CUESTA PASTOR, 2002: 43, 71. CORCOY BIDASOLO, 1999: 247-248. MENDOZA BUERGO, 2001: 18.

[234] RODRIGUEZ MOURULLO, 145 VARGAS PINTO, 2007: 136.

La protección de tales bienes se hace de forma mediata a través del adelantamiento de la tutela penal y la creación de un bien jurídico-penal de carácter supraindividual o colectivo: la seguridad informática, cuya lesión actuará como barrera de salvaguarda de tales intereses jurídicos[235]. La seguridad informática actuará como bien jurídico inmediatamente protegido y será referente para todos y cada uno de los bienes individuales, pero también colectivos como la propiedad intelectual, hecho que, sin duda, constituye una novedad única de este delito[236]. Sin embargo, el bien jurídico supraindividual seguridad informática tiene, como se ha visto, no un mero carácter formal, sino también un contenido material que es el que, en definitiva, le otorga al delito su identidad[237].

---

[235] CUESTA PASTOR, 2002: 89. MATA Y MARTÍN, 1997: 41-45, 49, 56, 82, 85-88. VARGAS PINTO, 2007: 39.

[236] CUESTA PASTOR, 2002: 89.

[237] Ello no supone tampoco que niegue la existencia de lo que se han denominado bienes jurídicos difusos o supraindividuales sin un referente individual, cuestión ésta que, en cualquier caso, no es objeto de este estudio. Se manifiestan a favor de la referencia mediata de los bienes jurídicos supraindividuales a bienes individuales CARBONELL MATEU, 1994: 16 y ss.. PORTILLA CONTRERAS, 1989: 745.. TERRADILLOS BASOCO, 2001: 805 y ss.. MAYO CALDERÓN, 2005: 56 nota 217.. No considero en ningún caso estemos ante la presencia de lo que se ha venido a denominar por MATA Y MARTÍN bien jurídico intermedio, en el que el bien jurídico colectivo tiene un carácter puramente formal y su legitimación se cimienta en que se halla vinculado al individual por una relación de medio-fin, careciendo de otro contenido que el de adelantar la barrera de punición de éste como forma de protección del mismo. Sin embargo, es cierto que en esta concepción de lesión-peligro -lesión del bien jurídico supraindividual y mera puesta en peligro del bien jurídico individual- tiene cierta aplicación en el presente supuesto, puesto que la lesión del bien jurídico colectivo será paso previo necesario para la puesta en peligro o, incluso, la lesión del bien jurídico individual. Algo que, no obstante, a mi juicio, sucederá en todos los casos en los que nos hallemos ante un bien jurídico supraindividual con un claro referente individual. MATA Y MARTÍN, 1997: 32. MAYO CALDERÓN, 2005: 56.

F) PROPUESTA DE REUBICACIÓN DEL DELITO CONFORME AL BIEN JURÍDICO PROTEGIDO SEGURIDAD INFORMÁTICA

Teniendo en cuenta todas las consideraciones vertidas hasta el momento, creo que el el Capítulo I del Título X no era el lugar más idóneo para ubicar el delito de acceso ilícito a un sistema informático[238]. Cuando menos, como indica MORALES PRATS, hubiera sido más aconsejable la creación de un capítulo independiente en el Título X, algo que hubiera ahorrado no todos pero sí algunos de los problemas interpretativos más importantes que se han planteado[239].

Sin perjuicio de resaltar que la actual no me parece la ubicación adecuada[240], tampoco creo que sea necesario crear un título autónomo para incluir únicamente el delito de acceso ilícito a un sistema informático, tal y como proponen algunos autores, que amparan esta idea en que así se reflejaría el carácter transversal del adelantamiento de la intervención del Derecho penal[241]. Esta opción se sitúa, en mi opinión —que en este caso sigue a la de MORALES PRATS—, al servicio de la creación de un Título dedicado a los delitos informáticos, los cuales, como se sabe, carecen de identidad propia, se encuentran desanclados del principio de lesividad y de la identificación clara de los bienes jurídicos a proteger[242], que en la mayor parte de ocasiones son los propios intereses tradicionales.

---

238 Como ponen de relieve ANARTE BORRALLO y DOVAL PAIS, resulta incongruente aplicar unos preceptos que aparecen dentro de la intimidad a casos en los que están en juego otro tipo de intereses, como los empresariales, institucionales o políticos, lo que genera un notable descuadre normativo respecto de las normas protegen los bienes jurídicos vinculados a éstos, como es el caso del secreto de empresa. ANARTE BORRALLO y DOVAL PAÍS, 2015: 513.

239 MORALES PRATS, 2011b: 820.

240 Y que, por el momento, no sea desacertada como proponen ANARTE BORRALLO y DOVAL PAIS una interpretación del tipo más apegada a la dimensión sistemática del precepto en tanto forma anticipada de tutela de la intimidad. ANARTE BORRALLO y DOVAL PAÍS, 2015: 513.

241 SÁNCHEZ DOMINGO, 2012: 38.

242 MORALES PRATS, 2011b: 820.

Por el contrario, creo que el acceso ilícito debería introducirse como una nueva categoría dentro de los delitos contra la seguridad colectiva, puesto que la estructura planteada responde perfectamente a este conjunto de delitos[243]. Con la protección y afianzamiento de la seguridad colectiva se trata de garantizar otros bienes[244]. La seguridad colectiva adquiere relevancia como bien jurídico individual penalmente protegido en la medida en que sirve para la protección de bienes jurídicos individuales, respecto de conductas que los ponen en peligro más allá de lo permitido[245]. Y es la protección penal de estos bienes jurídicos individuales lo que en definitiva hace merecedora de sanción penal la conducta, más allá de la pretendida sustantividad o autonomía de la seguridad colectiva como bien jurídico penalmente protegido[246]. En este sentido, GONZALEZ RUS define la seguridad colectiva como *el conjunto de condiciones cuyo cumplimiento asegura y genera la expectativa social de que no se incrementará el riesgo para los bienes personales o colectivos que se ven implicados en algunas actividades peligrosas mas allá de lo que es consustancial y permitido en cada una de ellas*[247].

---

[243] Respecto de los delitos de riesgo catastrófico MORALES PRATS y GARCÍA SOLÉ analizan cuál ha sido la opción del legislador: si tutelar los bienes jurídicos individuales que pudieran verse en último término afectados por estos delitos, o si este aspecto individual ha trascendido pretendiéndose tutelar un conjunto de condiciones necesarias para garantizar un determinado estándar de seguridad colectiva en el ámbito de actividad analizado, de modo que el bien jurídico adquiera una connotación institucional o colectiva (supraindividual). A tal efecto, manifiestan que, mediatamente, puede afirmarse que en estos delitos se halla comprometida la defensa de intereses de carácter personal, pero que su objeto no se agota en la suma de los mismos, sino en las condiciones que permiten asegurar su indemnidad como objeto diferenciado y anticipado de tutela. Consideran, en este sentido, que, como bien jurídico, junto a los intereses individuales protegidos, se puede percibir algo más que los trasciende y que se podría definir como el derecho que todos tienen para el desenvolvimiento normal de sus vidas en paz, sosiego, bienestar y tranquilidad. MORALES PRATS y GARCÍA SOLÉ, 2010: 1367-1368.

[244] TRAPERO BARREALES, 2006: 76-77.

[245] TRAPERO BARREALES, 2006: 70.

[246] TRAPERO BARREALES, 2006: 70-71.

[247] GONZALEZ RUS, 2011

A esta caracterización se adapta perfectamente, en mi opinión, conforme lo que se ha estudiado el delito de acceso ilícito, que es un medio adecuado para lograr el conjunto de condiciones necesarias para la utilización lícita de las nuevas tecnologías.

CAPITULO IV
CONDUCTAS TÍPICAS

I. INTRODUCCIÓN

Con el presente Capítulo se inicia el estudio de los elementos típicos del delito. De entre ellos el primero que se tratará y que, además, será objeto del presente Capítulo es la conducta típica. Tal y como se detalla a continuación, ésta se ha mantenido prácticamente inalterada por lo que respecta a la acción desde su introducción en el Código penal en 2010:

> a) La Ley Orgánica 5/2010, de 22 de junio, al introducir la conducta en el seno del artículo 197, previó un tipo mixto alternativo compuesto por dos acciones con distinto objeto material: la de acceder a datos y la de mantenerse en el sistema.
>
> b) La reforma operada Ley Orgánica 1/2015, de 30 de marzo, ha mantenido inalteradas ambas acciones —aunque ha cambiado el objeto material de la primera, que ahora es el sistema como se verá en el Capítulo V—, pero ha añadido una nueva modalidad alternativa al acceso: su facilitación.

Teniendo en cuenta la nimiedad de las modificaciones llevadas a cabo por la última reforma en relación con la acción típica, considero más apropiado para la presentación del presente capítulo su tratamiento conjunto, sin necesidad de establecer apartados separados de cada una de las redacciones, ya que solo se trata de adicionar la facilitación como una modalidad de comisión alternativa en la conducta de acceso.

Este capítulo se dedicará, por tanto, al estudio de las tres acciones típicas que integran la conducta del tipo penal objeto de análisis en el presente estudio: las de acceso, facilitación del acceso y mantenimiento ilícito en el sistema. El Capítulo se dividirá, en cambio, solo en dos Secciones teniendo en cuenta la estrecha vinculación existente entre las dos primeras. Así pues, la Sección 1ª estará dedicada al acceso y a su facilitación mientras que la Sección 2ª irá dirigida a estudiar la conducta de mantenimiento.

En cualquier caso, no es posible soslayar tampoco el estudio de la interacción de las distintas acciones en su conjunto en el propio tipo penal, motivo por el cual, antes que nada, será necesario ver como se articulan cada una de ellas en el delito y cuál es la relación existente entre ellas. A esto último se dedicarán, brevemente, las dos siguientes páginas.

II. CONFIGURACIÓN DE LAS CONDUCTAS

El acceso se introdujo *ex novo* a través de la Ley Orgánica 5/2010, de 22 de junio, pues, como un nuevo apartado 3 del artículo 197 del Código penal, previéndose en su descripción un tipo mixto alternativo compuesto de dos conductas: el acceso a datos o programas contenidos en un sistema informático o en parte del mismo, y el mantenimiento en dicho sistema en contra de la voluntad de quien tenga el legítimo derecho a excluirlo. Sin embargo, el objeto material del delito era distinto en cada conducta, lo que generaba importantes dificultades en relación con la aplicación del tipo.

A través de la reforma operada por la Ley Orgánica 1/2015, de 30 de marzo, esta incongruencia típica se ha corregido, siendo hoy en ambas el elemento sobre el que recae la acción el sistema informático. Hoy se trata, como anuncia el propio tipo al incluir la conjunción disyuntiva "o", de un tipo mixto alternativo cuya culminación tendrá lugar cuando se produzca cualquiera de las dos acciones que en él se describen —esto es, tanto la de acceso como la de mantenimiento—[1]. Lo anterior es expresado por la doctrina mediante dos consecuencias, desde un punto de vista[2]: a) Positivo: la perpetración de una de las accesiones previstas en el tipo para que la conducta sea típica y, al mismo tiempo, b) Negativo: la realización de ambas acciones dará lugar a responsabilidad por un solo delito de acceso ilícito.

Aún así, cabe resaltar que yerra la Ley al atribuir una estructura mixta acumulativa al presente tipo penal, pues parece que para poder realizar la acción de mantenimiento es necesario haber accedido con carácter previo de forma ilícita al sistema cuando esta modalidad debe ser típica solo en el caso contrario, esto es, cuando se ha accedido al sistema de forma lícita. Debería tratarse, pues de un tipo mixto alternativo en sentido estricto[3].

---

[1] Subrayan esta característica, PECORELLA, 2006: 349. DESTITO et al., 2007: 87. PICA, 1999: 42.

[2] ROMEO CASABONA, 2004b: 120.

[3] En similar sentido sobre propiedad intelectual LATORRE LATORRE, 2014: 98.

SECCIÓN 1ª

LA ACCIÓN DE ACCEDER Y FACILITAR EL ACCESO EN EL APARTADO 1 DEL ARTÍCULO 197 BIS DEL CÓDIGO PENAL

I. INTRODUCCIÓN

La primera de las dos conductas castigadas en el artículo 197.1 *bis* es el acceso o la facilitación del mismo al conjunto o a parte del sistema informático —acceso a datos o programas contenidos en todo o en parte de un sistema informático según la redacción vigente entre 2010 y 2015—. Como bien se observa, en esta modalidad comisiva la acción típica viene determinada por el verbo acceder, término que a su vez es empleado en multitud de preceptos a lo largo del Código penal para describir la acción punible. En este sentido, aunque la conducta de acceso ilícito a un sistema informático es relativamente nueva en nuestro Código penal, en realidad el verbo empleado para describirla no es nuevo ni siquiera en el seno del propio delito de descubrimiento y revelación de secretos, donde constituye uno de los seis comportamientos típicos que alternativamente prevé el apartado 2 del artículo 197.

Teniendo en cuenta la inmejorable oportunidad hermenéutica que dicho apartado brinda, considero adecuado ahondar antes que nada en qué debe entenderse por acceso en delito de descubrimiento y revelación de secretos. Además, a los motivos esbozados se une uno más, y es que, como cabe recordar, con la reforma de 2010 el acceso ilícito formaba parte de dicho delito, estando ubicado en el apartado inmediatamente subsiguiente al que se presenta como objeto de estudio, el apartado 2. De hecho, el delito de acceso ilícito no se ha ido muy lejos de su antigua ubicación, permanece en el artículo 197 *bis*.

Las razones apuntadas conducen a la necesidad de abrir una Subsección dentro de la presente Sección para analizar, en primer lugar, la conducta de acceso en el seno del artículo 197 del Código penal, —antigua ubicación del delito de acceso ilícito y, hoy, término sistemático comparativo para la interpretación del mismo, con el que sigue compartiendo Título y Capítulo—, para después entrar ya en el estudio detallado del concepto de acceso en la nueva conducta, al que se dedicará la Subsección 2ª.

SUBSECCIÓN 1ª

EL CONCEPTO DE ACCESO EN EL SENO DEL DELITO DE DESCUBRIMIENTO Y REVELACIÓN DE SECRETOS

I. INTRODUCCIÓN

Como se ha indicado, el término acceder se ha utilizado para describir uno de los seis comportamientos típicos que alternativamente prevé el apartado 2 del artículo 197. Siendo que dicho apartado compartió ubicación sistemática con el delito de acceso ilícito desde 2010 a 2015 y que, hoy, sigue compartiendo Título y Capítulo con el mismo, necesariamente debe utilizarse como término sistemático comparativo para su interpretación del mismo.

En general, la doctrina española ha encontrado serias dificultades a la hora de determinar el ámbito de aplicación de cada una de las modalidades típicas previstas en dicho precepto, debido, particularmente, a la proximidad de los difusos contornos entre algunos de los comportamientos en él castigados[4]. En este contexto, uno de los aspectos más problemáticos ha sido la delimitación de las acciones de acceso y apoderamiento —yuxtapuestas ambas en el apartado 2 de dicho precepto, aunque recogida específicamente la segunda en el apartado 1 del mismo—, que un sector de la doctrina ha llegado a considerar, incluso, conceptos equivalentes. Por consiguiente, se presenta como cuestión ineludible el esclarecimiento de qué debe entenderse por apoderarse en este tipo penal para, posteriormente, deslindar de ésta conducta el comportamiento de acceso. Este análisis ocupará el presente epígrafe.

---

[4] En efecto, la extrema confusión terminológica de la redacción típica es el principal defecto que la doctrina atribuye de forma unánime a este tipo penal (muy especialmente, por lo que se refiere al apartado 2), a causa del castigo con igual pena de conductas con distinto desvalor, de la reiteración y, cuando no, proximidad de las distintas conductas recogidas y, como indica ANARTE BORRALLO, por una suerte de incomodidad que el legislador parece manifestar hacia los elementos tecnológicos. ANARTE BORRALLO, 2001: 52. DE LA MATA BARRANCO, 2007: 63. DE LA MATA BARRANCO y HERNÁNDEZ DÍAZ, 2010: 176. DOVAL PAÍS, 2000: 98. HUERTA TOCILDO y ANDRÉS DOMÍNGUEZ, 2002: 65. JAREÑO LEAL, 2008: 24-25. JORGE BARREIRO, 2002: 100, 117. MATA Y MARTÍN, 2001: 140. MORALES PRATS, 2011: 454. ROMEO CASABONA, 2004b: 83, 115. ROMEO CASABONA, 2004a: 754. TOMÁS - VALIENTE LANUZA, 2010: 794, 801.

II. APODERAMIENTO VS. ACCESO EN EL DELITO DE DESCUBRIMIENTO Y REVELACIÓN DE SECRETOS

La acción de apoderamiento, que aparece recogida tanto en el apartado 1 como en el 2 del artículo 197 del Código penal, es considerada por la doctrina como el instrumento típico más adecuado para la incriminación de los delitos contra la intimidad[5]. La razón que se arguye al efecto es que el uso de este verbo está justificado si se atiende al carácter heterogéneo de los soportes a los que dicha acción va referida[6]. Sin perjuicio de lo anterior, la definición de qué debe entenderse como tal no está exenta de dificultades[7], cuestionándose multitud de aspectos salvo el hecho de que debe dársele una significación unívoca en ambas previsiones típicas[8].

A) DEFINICIÓN DEL CONCEPTO DE APODERAMIENTO

A los efectos de definir qué debe entenderse por apoderamiento pueden distinguirse en la doctrina dos grandes posturas, cuyo eje de diferenciación se cimienta en la naturaleza que cada una de ellas atribuye a dicho concepto. La diferencia más sustancial entre optar por una y otra tesis radica en que sobre ello pivotará el entendimiento de la consumación del delito y de los diversos factores concernientes a la misma. A continuación se presentarán cada una de estas teorías por separado:

---

[5] Por supuesto, algunos autores critican la difícil vinculación entre el verbo apoderar y los datos personales, cuya aprehensibilidad, en su opinión, no es posible y aducen la existencia de otros verbos más ajustados a los mismos. GÓMEZ NAVAJAS, 2005: 136. JAREÑO LEAL, 2008: 58. A favor, OLMO FERNÁNDEZ-DELGADO, 2009: 73.

[6] ORTS BERENGUER y ROIG TORRES, 2001: 25.

[7] Esta expresión proviene de la regulación contenida en el artículo 497 y 497 *bis* del Código penal de 1973, respecto de la cual existían ya serios problemas interpretativos en torno a este concepto, problemas que se mantienen todavía hoy y a los que se unen los propios de la adaptación y ampliación de su ámbito aplicativo. RODRÍGUEZ MORO, 2011: 243. ROMEO CASABONA, 2004b: 83-84.

[8] ORTS BERENGUER y ROIG TORRES, 2001: 31. POLAINO NAVARRETE, 1997: 401-402. RUIZ MARCO, 1999: 194.

1. TESIS PATRIMONIALISTA

La primera de estas posturas atribuye al apoderamiento una naturaleza de corte patrimonialista, propugnando su interpretación conforme al sentido que tradicionalmente se ha atribuido a este concepto en los delitos contra el patrimonio. Como es sobradamente sabido, la característica principal de los delitos patrimoniales de apoderamiento es la existencia de una traslación material de una cosa mueble del sujeto pasivo a la esfera de disponibilidad del sujeto activo[9], siendo la utilización de unos u otros medios comisivos determinados lo que conduce a su encaje en una u otra figura delictiva[10].

Los defensores de esta teoría en el ámbito del delito que nos ocupa consideran, por tanto, que el concepto de apoderamiento debe interpretarse también en el seno del delito de descubrimiento y revelación de secretos dándole esta misma significación material de apropiación, exigiendo en todo caso la existencia de un desplazamiento físico del contenido íntimo a la esfera de disponibilidad del sujeto activo[11].

---

[9] Aunque el término apoderamiento se usa solamente en la descripción típica del delito de robo, en general, la doctrina y la jurisprudencia atribuyen una significación conjunta a las distintas acciones enunciadas en los tipos penales de apoderamiento relativos al patrimonio, describiéndolas como el desplazamiento físico de las cosas del patrimonio del sujeto pasivo al del sujeto activo en los delitos de hurto y robo, aunque entendiendo que dicha traslación se produce en un sentido ideal en el de los tipos dedicados a la extorsión y a la usurpación. Por todos, MUÑOZ CONDE, 2015: 328.

[10] Efectivamente, con ello se pretende resaltar la existencia de un mayor contenido de injusto basado en la necesidad de sobrepasar las superiores barreras de protección existentes para conseguir el apoderamiento de la cosa.

[11] **a) En la doctrina:** ANARTE BORRALLO, 2001: 54. CALDERÓN y CHOCLÁN MONTALVO, 1999: 146. CARBONELL MATEU y GONZÁLEZ CUSSAC, 2010: CD 1. CASTIÑEIRA PALOU, 2010: 149. DE LA MATA BARRANCO, 2007: 63. DE LA MATA BARRANCO y HERNÁNDEZ DÍAZ, 2010: 176. DOVAL PAÍS, 2000: 93. FLORES PRADA, 2012: 63. JORGE BARREIRO, 1997: 573. JORGE BARREIRO, 2002: 102, 119. JORGE BARREIRO, 2011: 865 párrafo 9880. LOZANO MIRALLES, 1998b: 215. MATA Y MARTÍN, 2001: 128. MATA Y MARTÍN, 2006: 224. MUÑOZ CONDE, 2010: 273. OLMO FERNÁNDEZ-DELGADO, 2009: 78-79. ORTS BERENGUER y ROIG TORRES, 2001: 26. QUERALT JIMÉNEZ, 2010: 294. Dudoso, REBOLLO VARGAS, 2004: 456-457. Respecto del artículo 197.2 ROMEO CASABONA, 2004b: 120. **b) En la jurisprudencia:** STS 358/2007, 30 abril, 1219/2004, 10 dic FJ 8 STS 694/2003, 29 junio y la 367/2001, 22 marzo.

El apoderamiento se equipara, en consecuencia, a la posesión o tenencia del objeto[12], de carácter actual[13], que otorga al sujeto el dominio o control sobre éste y que le sitúa en la condición de acceder a su contenido, sin que sea necesario que esta circunstancia se produzca[14]. Esta posesión puede ser detentada por el sujeto como consecuencia de una actuación propia previa de adquisición subrepticia del objeto (arrebatar[15]) o derivada de una acción positiva de dominio tras la recepción accidental del mismo (retención de lo recibido por error)[16]. Pero a pesar de estas similitudes entre ambos conceptos de apoderamiento, no existe, por supuesto, plena identidad entre ellos, lo que se manifiesta en tres aspectos:

> **a) Medios comisivos:** el procedimiento empleado para apoderarse del objeto que contiene la intimidad es de todo punto irrelevante en el delito de descubrimiento y revelación de secretos[17], siendo típicos aquellos supuestos de apoderamiento en los que el titular ha olvidado o ha dejado el soporte al alcance de terceros[18] o cuando se desconozca cómo ha llegado éste al poder del sujeto activo[19].

---

[12] JAREÑO LEAL, 2008: 36.

[13] ORTS BERENGUER y ROIG TORRES, 2001: 31.

[14] MATA Y MARTÍN, 2006: 225.

[15] Esta exigencia relativa al carácter anterior de la acción de apropiación del sujeto permite delimitar con gran exactitud el *iter criminis* y, con ello, excluir de la tipicidad aquellos supuestos en los que el apoderamiento se produce con carácter posterior, esto es, una vez desvelada la información relativa a la intimidad. En consecuencia, la conducta queda acertadamente acotada a aquellos casos en los que el sujeto activo se apodera del objeto de forma subrepticia con el objetivo de poder después acceder a su contenido y, así, conocer datos relativos a la intimidad del sujeto pasivo. DOVAL PAÍS, 2000: 93. JORGE BARREIRO, 2002: 102. JORGE BARREIRO, 1997: 566.

[16] ANARTE BORRALLO, 2001: 54. CARBONELL MATEU y GONZÁLEZ CUSSAC, 2010: CD pág. 1. GONZÁLEZ RUS, 2011: 305.

[17] En contra DOVAL PAIS añade como exigencia el quebrantamiento de algún resguardo del sistema para llegar al mensaje. DOVAL PAÍS, 2000: 93. A favor, QUERALT JIMÉNEZ, 2010: 294.

[18] (SAP Alicante, 74/1999, 22 marzo)

[19] JAREÑO LEAL, 2008: 36.

b) Objeto material: la exigencia de una aprehensión material, supone en todo caso un desplazamiento, pero este desplazamiento se sustancia de forma diferente al delito de descubrimiento y revelación de secretos:

aa) Aprehensión física: la interpretación tradicional exige un acto de aprehensión física del soporte que conduzca a la consiguiente desposesión de éste del sujeto pasivo[20].

bb) Aprehensión virtual: en aras de adaptar el concepto de apoderamiento a los avances de la informática, se ha prescindido de exigir la aprehensión del soporte físico que contiene la intimidad, centrando la atención en la efectiva apropiación del archivo informático que la contiene, conducta que se considera idónea para colmar el tipo. De este modo, apoderamiento ya no supone privar al sujeto pasivo de la posesión del soporte físico original, siendo perfectamente factible, pues, que ni siquiera se de desplazamiento de éste[21], teniendo simplemente lugar la traslación de la información, de carácter intangible, a otro soporte, éste forzosamente tangible, mediante su reproducción a través del fotocopiado, fotografiado, envío telemático, la impresión o la transmisión del archivo a un dispositivo informático[22].

---

[20] ANARTE BORRALLO, 2001: 54. CARBONELL MATEU y GONZÁLEZ CUSSAC, 2010: CD pág. 1. QUERALT JIMÉNEZ, 2010: 294.

[21] CALDERÓN y CHOCLÁN MONTALVO, 1999: 133.

[22] Hoy día, se considera que satisface una interpretación gramatical y sistemática del precepto el entendimiento de que la característica definitoria del apoderamiento es la tenencia: apoderar significa que el sujeto activo ha conseguido el contenido íntimo para sí. *de cualquier forma técnica que permita su reproducción posterior, como por ejemplo mediante su fotografiado.* Como muy bien indica DOVAL PAIS en este caso la reproducción *resulta completamente fiel al documento original y puede merecer mayor credibilidad si se revelase, difundiese o cediese que una mera manifestación del mensaje que fue visto y retenido mentalmente.* STS 14 septiembre 2000 CASTIÑEIRA PALOU, 2010: 149. DE LA MATA BARRANCO, 2007: 63. DE LA MATA BARRANCO y HERNÁNDEZ DÍAZ, 2010: 176. MATA Y MARTÍN, 2001: 129. MATA Y MARTÍN, 2006: 224. ORTS BERENGUER y ROIG TORRES, 2001: 26. JORGE BARREIRO, 2002: 102, 119. DOVAL PAÍS, 2000: 94.

c) Orientación subjetiva: el apoderamiento opera en la dinámica de la conducta típica en tanto *instrumentum sceleris* de la comisión delictiva a los efectos de cumplir la finalidad tendencial de la conducta del sujeto activo, esto es, acceder a la información íntima en el apartado 1 y ocasionar un perjuicio ajeno en el apartado 2.

aa) Apartado 1 del artículo 197: En este apartado el elemento subjetivo del delito se contiene en los incisos *para descubrir los secretos* y *vulnerar la intimidad de otro*. Un grupo muy reducido de autores considera que en ellos se realiza una alusión directa al dolo[23], propugnando la eliminación de la primera referencia (*para descubrir los secretos*)[24]. Doctrina prácticamente unánime, en cambio, conviene en que ambos expresan el elemento subjetivo tendencial del apoderamiento, erigiéndolo en el elemento nuclear del injusto y definiéndolo como el potencial descubrimiento de información íntima (posibilidad de conocimiento) sin que ello implique, en ningún caso, el conocimiento efectivo de la misma[25]. Desde esta perspectiva el descubrimiento cumpliría simplemente una función de engarce entre el tipo básico del apartado 1 y el tipo agravado de difusión o revelación del apartado 4[26].

---

[23] Por el contrario, ANARTE BORRALLO entiende que el descubrimiento sólo puede servir de engarce cuando éste forma parte del tipo penal y no cuando se considera únicamente como un elemento subjetivo del injusto. ANARTE BORRALLO, 2001: 54-55.

[24] Por todos MORALES PRATS, 2011: 456.

[25] MANZANARES SAMANIEGO y MUÑOZ CONDE consideran que encierra una doble intencionalidad: por una parte la de conocer y, por otra, la de revelar MORALES PRATS, 2011: 455. CALDERÓN y CHOCLÁN MONTALVO, 1999: 133. CARBONELL MATEU y GONZÁLEZ CUSSAC, 2010: CD pág. 2. COBO DEL ROSAL, 1971: 681. DE LA MATA BARRANCO, 2007: 62. DE LA MATA BARRANCO y HERNÁNDEZ DÍAZ, 2010: 175. MANZANARES SAMANIEGO, 1978: 311. MATA Y MARTÍN, 2001: 128. MUÑOZ CONDE, 2015: 236. POLAINO NAVARRETE, 1997: 399. ROMEO CASABONA, 2004b: 84. REBOLLO VARGAS, 2004: 457.

[26] MATA Y MARTÍN, 2001: 129.

bb) Apartado 2 del artículo 197: Aquí el elemento subjetivo consiste en perjudicar *a un tercero* (primer inciso) o *al titular de los datos o un tercero* (segundo inciso). La doctrina ha discutido acerca de cómo debe interpretarse este inciso[27], manejando varias hipótesis al respecto: algunos autores interpretan que perjudicar es el efecto de descubrir, el cual puede o bien integrarse por el propio conocimiento de los datos personales o bien derivarse de éste[28]; otros centran la atención en la vulneración de la intimidad y excluyen de él el efectivo conocimiento de los datos personales, ya sea como elemento objetivo resultado del delito[29] o subjetivo[30]; finalmente, una posición más abierta esgrime que tan solo expresa la tendencia subjetiva interna del autor de cometer el delito con independencia, también, de que se logre conocimiento sobre los datos[31].

---

[27] Son diversas y de gran complejidad las cuestiones que han resultado controvertidas en torno a la interpretación de estas expresiones: desde la implicación de los distintos sujetos a los que se hace alusión, hasta la propia naturaleza de la cláusula objeto de comentario. DOVAL PAÍS, 2000: 102-103. GONZÁLEZ RUS, 2011: 316-317.

[28] MORÓN LERMA, 2001: 1626. HUERTA TOCILDO y ANDRÉS DOMÍNGUEZ, 2002: 64.

[29] JAREÑO LEAL y DOVAL PAIS sugieren que, aunque este elemento en realidad no aporta nada (se limita a expresar el resultado de la conducta: que una vez realizada la acción se verifica la lesión del bien jurídico), su inclusión cobra pleno sentido en tanto cláusula de limitación del alcance del tipo frente a comportamientos que no suponen un perjuicio para la intimidad. En un sentido similar, GÓMEZ LANZ entiende que su misión es dotar de una mayor ofensividad a las conductas que solo suponen un peligro para el bien jurídico. Se añade a lo anterior que ello impide la concurrencia de otros ánimos, como por ejemplo la obtención de un beneficio económico o el mero ánimo de quebrantar los sistemas de seguridad que protegen los datos. DOVAL PAÍS, 2000: 102. DOVAL PAÍS y JAREÑO LEAL, 2000: 4. GÓMEZ LANZ, 2006: 254. HUERTA TOCILDO y ANDRÉS DOMÍNGUEZ, 2002: 25, 64.

[30] Sin más precisiones MUÑOZ CONDE, 2015: 237. QUERALT JIMÉNEZ, 2010: 301. REBOLLO VARGAS, 2004: 468. CASTIÑEIRA PALOU, 2010: 148.

[31] ORTS BERENGUER Y ROIG TORRES consideran que puesto que el número de conductas castigadas en el segundo apartado del precepto es más amplio que el primero, una interpretación sistemática del mismo conduce forzosamente a ampliar también el espectro del elemento subjetivo del injusto. ORTS BERENGUER y ROIG TORRES, 2001: 39-40.

Como se ha expuesto, de acuerdo con los postulados de esta teoría, el elemento nuclear del apoderamiento es la aprehensión física de un objeto que contiene o expresa la intimidad. Ésta tiene lugar, por tanto, cuando se traslada el contenido íntimo (todo o parte de él, pero, en todo caso, aspectos relevantes para la intimidad[32]) al ámbito de **disponibilidad** del sujeto activo mediante un soporte, propio o ajeno, que permita obtener el control sobre el mismo[33]. Disponibilidad implica, en este sentido, capacidad para acceder al conocimiento de la información personal contenida en el soporte[34], y se expresa en la ejecución de un acto positivo de dominio sobre el objeto que la contiene una vez que ésta ha llegado a su esfera de acción, ello con independencia de que la acción de apoderamiento haya sido realizada por el propio sujeto activo o por un tercero que coopere con él[35]. Concretamente, la disponibilidad sobre el objeto se puede adquirir de dos formas[36]:

> **a) Atracción de éste por parte del sujeto activo a su ámbito de dominio o control:** el sujeto está capacitado para acceder al contenido íntimo porque dispone de un objeto material que lo contiene o expresa y está en tal momento bajo su control[37].
>
> **b) Retención de lo recibido por error:** la conducta se integra no solo por la mera inactividad o pasividad del sujeto, sino por una acción positiva de éste, en tanto erróneo receptor, dirigida a lograr que dicho objeto quede bajo su dominio[38].

---

[32] DOVAL PAÍS, 2000: 94. MATA Y MARTÍN, 2001: 128.

[33] CASTIÑEIRA PALOU, 2010: 147.

[34] GONZÁLEZ RUS, 2005: 349.

[35] ROMEO CASABONA, 2004b: 84.

[36] A favor de ambas modalidades RUIZ MARCO, 1999: 113. ROMEO CASABONA, 2004b: 84-85. En contra de la tipicidad de la retención de lo recibido por error: ANARTE BORRALLO, 2001: 54. FERNÁNDEZ TERUELO, 2007: 124. GONZÁLEZ RUS, 2005: 349. MORANT VIDAL, 2003: 61. JORGE BARREIRO, 2002: 102.

[37] En sentido similar, ROMEO CASABONA, 2004b: 84.

[38] ROMEO CASABONA, 2004b: 84.

La **consumación** del delito se produce, precisamente, en este momento (el de la adquisición de la disponibilidad) presentándose el tipo, por tanto, para la mayor parte de los autores como un delito de resultado[39]. Además, también se define como un tipo mutilado de dos actos[40] y de consumación anticipada[41] en el que el acto de apoderamiento opera en la dinámica comisiva como un mero instrumento para cumplir la finalidad a la que tiende el sujeto activo, esto es, acceder al conocimiento de la información íntima[42].

Este potencial descubrimiento de información íntima —en tanto posibilidad de conocimiento pero en ningún caso como conocimiento efectivo[43]— implica la retroacción de la perfección del delito al momento en que se produce el apoderamiento, siendo que la efectiva consecución del descubrimiento de la intimidad o la causación del perjuicio pertenece a la fase de agotamiento del delito, aunque queda dentro de la esfera de dominio del sujeto[44].

---

[39] En contra, QUERALT JIMÉNEZ lo considera como un delito de resultado cortado. A favor, ORTS BERENGUER y ROIG TORRES, 2001: 31. QUERALT JIMÉNEZ, 2010: 301.

[40] QUERALT JIMÉNEZ, 2010: 301.

[41] ROMEO CASABONA, 2004b: 84.

[42] CALDERÓN y CHOCLÁN MONTALVO, 1999: 133. COBO DEL ROSAL, 1971: 681. MATA Y MARTÍN, 2001: 128. POLAINO NAVARRETE, 1997: 399. ROMEO CASABONA, 2004b: 84.

[43] En contra, ANARTE BORRALLO entiende, por el contrario, que adquiere mejor sentido *una versión más comprometida* de los verbos previstos en el tipo, lo que supone entender que las diversas acciones comportan el efectivo descubrimiento de la intimidad por parte del autor o autores. Ello también en aras a lo que denomina como necesaria coordinación que debe existir entre el número 1 y el número 2 con el número 3. Por este sentido, al igual que QUERALT JIMÉNEZ, interpreta como tentativa aquellos supuestos en los que el sujeto activo se apodera del soporte pero no llega a conocer la información, situando la barrera de la consumación no entre apoderamiento y descubrimiento un paso más allá, en la revelación una vez producido el apoderamiento y el descubrimiento. En coherencia con ello, sostiene que la referencia a vulnerar la intimidad no es más que la manifestación del dolo directo de primer grado, configurando así el delito como un delito de resultado lesión. COBO DEL ROSAL, 1971: 681. JORGE BARREIRO, 2002: 103.

[44] ROMEO CASABONA, 2004b: 84.

2. TESIS DE LA NORMATIVIZACIÓN O ESPIRITUALIZACIÓN

Otro sector de la doctrina, mayoritario en materia de secreto de empresa pero todavía minoritario por lo que respecta a los delitos contra la intimidad entiende que, debido a las especiales características de los elementos informáticos, la acepción clásica patrimonial del verbo apoderarse no resulta a aplicable a los mismos[45]. En este sentido, critica la concepción patrimonialista del término apoderamiento al considerarla contraria a la realidad actual y, por consiguiente, injustificable desde un punto de vista político-criminal[46]. Las razones que esgrimen estos autores pueden resumirse en tres:

> a) En primer lugar, desde un punto de vista teleológico consideran que el concepto tradicional de apoderamiento toma como punto de referencia el factor físico, lo que supone primar el objeto (el soporte) en detrimento del contenido (los datos íntimos), el cual en el campo de la intimidad constituye la única manifestación del bien jurídico[47].
>
> b) En segundo lugar, aducen un argumento gramatical basado en que si lo que se castigase fuera un apoderamiento meramente físico no se hubiera hecho alusión a los mensajes de correo electrónico y en que si éstos se han referenciado

---

[45] En el ámbito del secreto de empresa (artículo 278 del Código penal) la defensa de esta postura es dominante en la doctrina con base en la incorporiedad que se atribuye al secreto de empresa en tanto objeto material del delito.

a) Respecto delitos contra la intimidad: COBO DEL ROSAL, 1971: 699. FERNÁNDEZ TERUELO, 2007: 123. FERNÁNDEZ TERUELO, 2011: 190-191. GÓMEZ NAVAJAS, 2005: 138. GONZÁLEZ RUS, 2011: 305. JAREÑO LEAL, 2008: 36. MORANT VIDAL, 2003: 61. MORALES PRATS, 2011: 455. MORÓN LERMA, 2002a: 62. POLAINO NAVARRETE, 1997: 398, 402-403. RUEDA MARTÍN, 2004: 42-43, 77-78. RUIZ MARCO, 1999: 154-155, 159. RUIZ MARCO, 2001: 53.

b) Respecto delito contra el secreto de empresa: FARALDO CABANA, 2010: 1067. FERNÁNDEZ SÁNCHEZ, 2000: 232. MORALES PRATS y MORÓN LERMA, 2011: 862.. MORÓN LERMA, 2002b: 534-535. En contra, ORTS BERENGUER y ROIG TORRES, 2001: 105.

[46] RUIZ MARCO, 1999: 54.

[47] MATA Y MARTÍN, 2001: 127-128.

expresamente es porque el apoderamiento no puede quedar limitado a un sentido meramente material o físico, el cual no se correspondería con *el estado natural de estos mensajes* (virtual) *sin ningún soporte material que los contenga,* ya que, además, impresos en papel, los correos electrónicos se convertirían en simples papeles, cartas o documentos[48].

c) En tercer y último lugar, sistemáticamente, entienden que, mientras en los delitos contra el patrimonio la lesión del bien jurídico viene representada por la privación al sujeto del objeto material, ello no es necesario para la afectación de la intimidad porque tanto las comunicaciones privadas cuanto los datos personales se proyectan en documentos digitales, para cuyo acceso (y consiguiente injerencia en la intimidad) no se requiere apoderamiento físico alguno[49].

Tomando como punto de partida las consideraciones expuestas en las críticas transcritas, este sector doctrinal defiende que los **nuevos objetos materiales de carácter tecnológico** que se han incorporado en el Código penal de 1995 condicionan el significado del verbo apoderarse[50]. Interpretando, pues, que **la intangibilidad de estos elementos hace imposible su aprehensión física**, aboga por lo que se ha denominado un **concepto espiritualizado[51] o normativizado[52] de apoderamiento**. Ello supone conceptuar el apoderamiento como una **traslación posesoria cognitiva**[53] del contenido íntimo, esto es, el mero acceso intelectual o la captación visual del contenido íntimo de un soporte informático[54].

---

[48] RUEDA MARTÍN, 2004: 42-43.

[49] RUIZ MARCO, 1999: 154-156.

[50] JAREÑO LEAL, 2008: 36.

[51] ROMEO CASABONA, 2004b: 84.

[52] ANARTE BORRALLO, 2001: 54.

[53] RUIZ MARCO, 1999: 54.

[54] MORALES PRATS, 2011: 455.

Este apoderamiento cognitivo excluye, por tanto, que se produzca un previa aprehensión material del soporte que contiene la información o una traslación física del contenido íntimo a otro soporte. Conforme a esta idea, asimismo, son susceptibles de ser planteadas dos hipótesis[55]:

> **a) Remoción previa de algún obstáculo de acceso**: incluye aquellos supuestos en los que el sujeto activo necesita realizar un acto previo que le permita la visualización del contenido, consistente o bien en el quebrantamiento de las defensas dispuestas para impedir el acceso, o bien la acción electrónica de apertura del documento.
>
> **b) Acceso directo al contenido del soporte:** supone la mera visualización del contenido íntimo sin necesidad de remover ningún impedimento previo. En este punto, este sector doctrinal distingue por una parte la visualización (visión del texto) y, por otra parte, el acceso intelectual al contenido (lectura del contenido)[56].

La aceptación de ambos supuestos no es unánime en la doctrina, de manera que, mientras algunos autores se decantan por admitir ambos[57], otros consideran excesiva la desmaterialización a la que supone someter el concepto de apoderamiento en la segunda acepción y consideran admisible únicamente la primera[58].

---

[55] ROMEO CASABONA, 2004b: 86-87.

[56] Indica, además, RUIZ MARCO que el acceso intelectual no precisa en todos los casos el acceso físico al soporte que los contenga, lo que define como traslación posesoria cognitiva. FERNÁNDEZ TERUELO, 2011: 178. RUIZ MARCO, 2001: 53.

[57] Curiosamente, MORALES PRATS considera que el tipo debe referirse a apoderamiento físico subrepticio de documentos y a conductas de captación mental o intelectual sin desplazamiento ilícito, insertando en la conducta de interceptación los comportamientos típicos de interceptación, reproducción o grabación ilícita de carácter electrónico. FERNÁNDEZ TERUELO, 2011: 176. MORALES PRATS, 2011: 455. MORANT VIDAL, 2003: 61. RUIZ MARCO, 2001: 53.

[58] GONZÁLEZ RUS, 2011: 305. JAREÑO LEAL, 2008: 23, 46. ROMEO CASABONA, 2004b: 88 nota 29. RUEDA MARTÍN, 2004: 42-43, 77-78.

La determinación del **momento consumativo** por parte de los seguidores de esta tesis resulta extremadamente conflictiva, si bien la mayor parte de ellos llegan a un resultado similar al apuntado para la teoría anterior: entienden que se trata de un delito de mera actividad[59], mutilado de dos actos[60] y de consumación anticipada, en el que concurren como elementos subjetivos del injusto la intencionalidad de descubrir los secretos[61] o vulnerar la intimidad de otro, y el ánimo de causar un perjuicio, sin que sea necesario que efectivamente éste se produzca[62].

---

[59] ROMEO CASABONA lo concibe como un delito de peligro y, en consecuencia, de mera actividad. RUEDA MARTÍN considera que se trata de un delito de lesión, de intención y de resultado cortado en el que el apoderamiento tiene lugar con el fin de que se produzca un determinado resultado, que queda fuera del tipo y que se concreta en el descubrimiento de los secretos o la vulneración de la intimidad de otro. ROMEO CASABONA, 2004b: 99. RUEDA MARTÍN, 2004: 51, 81-82.

[60] MORALES PRATS califica este delito como un delito imperfecto mutilado de dos actos, esto es, un tipo penal de los denominados de estructura incongruente por exceso subjetivo, que no requiere para la consumación el efectivo descubrimiento de los documentos, papeles, cartas o mensajes. RUEDA MARTÍN estima que no se trata de un delito mutilado de dos actos y critica que el resultado de lesión del bien jurídico que se produciría con el descubrimiento efectivo del secreto o con la vulneración de la intimidad queda fuera del tipo y no sea necesario para que se produzca la consumación. JAREÑO LEAL, en conformidad con la integración de la exigencia de conocimiento para la consumación del tipo en tanto desvalor de resultado y, por tanto, la exclusión de la existencia de un elemento subjetivo del injusto, descarta que se trate de un delito mutilado de dos actos al considerar que supone un adelanto excesivo de la barrera punitiva. Defienden que se trata de un delito mutilados de dos actos: JAREÑO LEAL, 2008: 25. MORALES PRATS, 2011: 455-456. RUEDA MARTÍN, 2004: 51, 81-82. RUIZ MARCO, 2001: 55. ROMEO CASABONA, 2004b: 100.

[61] ROMEO CASABONA afirma que descubrir alude a la captación intelectual del contenido del soporte, a su conocimiento, pero en este caso tal captación ha de recaer sobre un secreto de carácter personal, esto es, sobre un hecho que su titular ha querido dejar fuera del alcance de los demás o tan sólo accesible a un número limitado de personas. ROMEO CASABONA, 2004b: 99-100. RUIZ MARCO, 1999: 55. MORALES PRATS, 2011: 457. ROMEO CASABONA, 2004a: 100. RUEDA MARTÍN, 2004: 52, 81-82. RUEDA MARTÍN, 2004: 52.

[62] Por su parte, JAREÑO LEAL considera que es necesario el conocimiento efectivo de la intimidad del sujeto pasivo, lo que denomina *la llegada real al dato personal*, siendo esta circunstancia la única capaz de producir la efectiva lesión de la intimidad y, en consecuencia, la única capaz de integrar el desvalor del resultado del delito, puesto que, si ello no se exigiese, el tipo se convertiría en un delito de carácter puramente formal que castigaría *el mero hecho de rebasar las defensas de la intimidad, aunque no se llegue a descubrir algo que pertenezca a ésta*. JAREÑO LEAL, 2008: 25. A favor, SUÁREZ-MIRA RODRÍGUEZ y PIÑOL RODRÍGUEZ, 2012: 169. ROMEO CASABONA, 2004b: 100. RUIZ MARCO, 1999: 154-155.

Como aportes que hace esta nueva teoría, destacan los defensores de esta tesis que con ella se palian dos de las importantes incongruencias del tipo penal:

> a) Por una parte, la desvinculación del elemento material de la acción de apoderamiento implica su equiparación a la conducta de acceso[63], hecho que permite la realización de una "lectura unitaria" de ambas conductas[64] y, con ello, se soluciona el escollo relativo la idéntica punición de diversas conductas con distinto desvalor de injusto[65].
>
> b) Por otra parte, esta misma característica permite a este sector doctrinal solucionar el conflicto que, para éste, se presenta en relación con la imposibilidad de aprehender datos íntimos de forma virtual[66].

De acuerdo con esta concepción, existiría una **equiparación plena entre apoderamiento y acceso**, que serían términos sinónimos, pues éste último se utiliza para definir el primero: el mero acceso al contenido del soporte ya integra el desvalor a que se refiere el apoderamiento. Debido a lo anterior, algunos autores se han referido al carácter superfluo de la modalidad de acceso[67], considerando al efecto que se trata de una innecesaria reduplicación de conductas[68].

El siguiente paso lo determinará, pues, profundizar en el concreto contenido y alcance de la conducta de acceso, lo que no impedirá, antes de ello, detenerse para ofrecer un posicionamiento crítico a favor de una u otra teoría.

---

[63] A la que se ha hecho referencia en el inicio de este apartado.

[64] ORTS BERENGUER y ROIG TORRES, 2001: 31.

[65] JAREÑO LEAL, 1999: 23-24.

[66] JAREÑO LEAL, 2008: 36. MATA Y MARTÍN, 2001: 127-128. RUIZ MARCO, 1999: 154-156.

[67] FERNÁNDEZ TERUELO, 2011: 190.

[68] MORÓN LERMA, 2002a: 62.

3. VALORACIÓN PERSONAL

De entre las dos tesis propuestas, me decanto por la primera de las teorías expuestas, la patrimonialista. El concepto de apoderamiento, al igual que el concepto de secreto, es un **elemento normativo del tipo de carácter social**, cuya valoración está plenamente vinculada a su sentido social[69]. El punto clave de este término es, sin duda, la idea de apropiación[70], cuyo significado está entroncado intrínsecamente a la idea de **adquisición o traslación posesoria**[71]. Resulta inviable, por tanto, la transfiguración del mismo mediante cualquier intento de juridificación, lo que le haría perder su significación.

El verdadero desvalor material de la acción de apoderamiento lo integra, para mí, la **aprehensión física** del objeto material del delito, que implica obtener una posesión directa e inmediata sobre contenido íntimo o un soporte que contiene o expresa la intimidad[72] y que permite al sujeto obtener una imagen fiel del documento original que puede reproducir posteriormente o que le puede otorgar un alto grado de credibilidad en caso de que proceda a su revelación, difusión o cesión[73]. Trasladado lo anterior al artículo 197, se trata de la ejecución por parte del sujeto activo de un acto destinado a obtener o retener un mensaje de correo electrónico, un documento electrónico o un efecto personal en el caso del apartado 1 del artículo 197 del Código penal[74], o un dato reservado de carácter personal o familiar contenido en un fichero o registro informático en el supuesto del apartado 2 de dicho precepto[75].

---

[69] MIR PUIG, 2005: 235-236 párrafos 66-71.

[70] Véase Apartado A) 1. a) de este epígrafe.

[71] ANARTE BORRALLO, 2001: 54.

[72] DOVAL PAÍS, 2000: 94.

[73] DOVAL PAÍS, 2000: 94.

[74] ORTS BERENGUER y ROIG TORRES, 2001: 26.

[75] OLMO FERNÁNDEZ-DELGADO, 2009: 78-79. ORTS BERENGUER y ROIG TORRES, 2001: 35.

La característica principal es la **obtención del contenido íntimo** y, mientras este requisito se cumpla, poco importan al Derecho penal los medios para su obtención o la forma en la que de ésta se disponga: papel o electrónica[76]. Es perfectamente factible para entender producida la aprehensión que ni siquiera se de un desplazamiento del soporte original que contiene la intimidad[77], teniendo simplemente lugar la traslación de contenido, de carácter intangible, a otro soporte, éste forzosamente tangible, mediante su reproducción a través del fotocopiado, fotografiado, envío telemático o la transmisión del archivo a un dispositivo informático, supuesto al que se ha hecho en ocasiones referencia como aprehensión virtual[78]. Ello conduce a subsumir en el tipo tanto la **aprehensión física como la virtual** en el sentido ya expresado anteriormente, pues ambas cumplen la condición mencionada: permitir al sujeto obtener una imagen fiel del contenido íntimo[79].

No pueden quedar englobadas, sin embargo, en esta idea de apropiación todas aquellas conductas que no llevan aparejada la materialización a la que se ha hecho referencia. Ello supone excluir del ámbito típico del delito un importante número de supuestos, concretamente los relativos al mero **acceso o visualización de la intimidad** contenida en formato electrónico, los cuales quedarían subsumidos en el tipo si se acepta la teoría de la normativización o espiritualización del concepto de apoderamiento. Y considero, además, que esta exclusión típica no ocasiona un especial trastorno al entramado típico desde el punto de vista del principio de ofensividad y legalidad, ello en aras a la seguridad jurídica[80].

---

[76] Véase Apartado A) 1. a) de este epígrafe.

[77] CALDERÓN y CHOCLÁN MONTALVO, 1999: 133.

[78] DE LA MATA BARRANCO, 2010: 176. DOVAL PAÍS, 2000: 93. ORTS BERENGUER y ROIG TORRES, 2001: 26. ROMEO CASABONA, 2004b: 85-120.

[79] Véase Apartado A) 1. a) de este epígrafe.

[80] Véase Apartado A) 1. a) de este epígrafe.

Por una parte, desde la perspectiva del **principio de ofensividad** porque para los seguidores de esta tesis el delito de descubrimiento y revelación de secretos es un delito mutilado de dos actos y de consumación anticipada (para algunos, cabe recordar, de resultado cortado) en el que el descubrimiento, entendido éste como conocimiento efectivo de la intimidad, no forma parte del tipo objetivo[81], siendo que su perfección se produce con el acto de apoderamiento, esto es, con la mera visualización del contenido íntimo[82].

Pues bien, entender producida la consumación en el momento en que el sujeto pone la vista encima del documento me parece no ya una desmaterialización desmesurada del concepto de apoderamiento[83] sino un adelantamiento excesivo de la barrera punitiva a un momento donde ni siquiera existe peligro para el bien jurídico protegido, lo que convierte al delito en un mero **delito obstáculo**, que castiga el peligro que puede suponer que alguien se acerque a, por ejemplo, un correo electrónico que un sujeto tiene abierto en la pantalla del ordenador[84]. Como muy acertadamente indican ORTS BERENGUER y ROIG TORRES se podría llegar a soluciones tan inverosímiles como la de aplicar una pena de prisión de hasta cuatro años a quien se limitase a leer mensajes, cartas, etc. que el interesado hubiese dejado al alcance de terceros[85].

---

[81] JAREÑO LEAL, 2008: 25. MORALES PRATS, 2011: 455-456. RUEDA MARTÍN, 2004: 51, 81-82. RUIZ MARCO, 2001: 55. ROMEO CASABONA, 2004b: 100.

[82] CALDERÓN y CHOCLÁN MONTALVO, 1999: 133. COBO DEL ROSAL, 1971: 681. GONZÁLEZ RUS, 2005: 348-349. MATA Y MARTÍN, 2001: 128. POLAINO NAVARRETE, 1997: 399. ROMEO CASABONA, 2004b: 84.

[83] GONZÁLEZ RUS, 2011: 305. JAREÑO LEAL, 2008: 23, 46. ROMEO CASABONA, 2004b: 88 nota 29. RUEDA MARTÍN, 2004: 42-43, 77-78.

[84] En mi opinión, resultaría menos lesivo del principio de ofensividad, como defiende un sector de la teoría de la espiritualización, retrasar la barrera punitiva hasta el momento en que se adquiere el conocimiento de los datos. Aunque ello supone la eliminación del elemento de intención del delito, permite al menos entender producida la afectación del bien jurídico intimidad. Esto dotaría de un mayor desvalor a la conducta, especialmente en el supuesto relativo a la remoción de un obstáculo previo, pero también a la mera visualización de los datos íntimos sin quebrantamiento de las barreras de defensa.

[85] ORTS BERENGUER y ROIG TORRES, 2001: 31.

Efectivamente, el apoderamiento opera en la dinámica comisiva del delito de descubrimiento y revelación de secretos como el ***instrumentum sceleris* de la comisión del delito**, en el sentido de que se produce únicamente para cumplir la finalidad a la que tiende la voluntad del sujeto activo[86]. Por tal razón, me parece acertado afirmar que el delito viene informado por un elemento subjetivo del injusto[87] integrado por el potencial descubrimiento de información íntima en tanto **posibilidad de conocimiento pero en ningún caso de conocimiento efectivo en el apartado 1**[88], y la intención de causar un perjuicio de cualquier clase en el apartado 2[89].

En coherencia con ello, considerando el delito como de peligro concreto (el bien jurídico intimidad es un derecho personalísimo de modo que el peligro se produce sólo en relación con la intimidad del sujeto víctima de la acción de apoderamiento), creo acertado afirmar que se trata de un delito de resultado, mutilado de dos actos y de consumación anticipada por lo siguiente:

> a) Es un **delito de resultado** porque se consuma cuando se adquiere la **disponibilidad** sobre todo o parte del contenido de un soporte que contiene aspectos relevantes para la intimidad[90], ya sea mediante una acción de arrebatar como de retener, pues ambas posibilidades son, a mi juicio, compatibles con la tesis expuesta[91]. Disponibilidad puede definirse, en este sentido, como la capacidad para conocer la información personal del sujeto pasivo[92].

---

[86] CALDERÓN y CHOCLÁN MONTALVO, 1999: 133. COBO DEL ROSAL, 1971: 681. GONZÁLEZ RUS, 2005: 348-349. MATA Y MARTÍN, 2001: 128. POLAINO NAVARRETE, 1997: 399. ROMEO CASABONA, 2004b: 84.

[87] MORALES PRATS, 2011: 455.

[88] COBO DEL ROSAL, 1971: 681.

[89] En el sentido ya expuesto.

[90] DOVAL PAÍS, 2000: 94. MATA Y MARTÍN, 2001: 128.

[91] ROMEO CASABONA, 2004b: 84.

[92] GONZÁLEZ RUS, 2005: 349.

b) Es un **delito mutilado de dos actos** y de **consumación anticipada** porque la intención de lesionar la intimidad es el elemento subjetivo del injusto que informa la realización de la conducta del sujeto activo pero no forma parte del tipo objetivo a los efectos de la perfección del delito[93]. La consumación, como se ha visto, se ha adelantado al momento en que se produce el apoderamiento sin que se requiera el efectivo descubrimiento de la intimidad o la causación del perjuicio. Este acto pertenecerá a la fase de agotamiento del delito, pero quedará dentro de la esfera de dominio del sujeto activo[94].

Por otra parte, desde el punto de vista del **principio de legalidad** también se pueden dar motivos de menor peso para fundar esta decisión. Así, razones de congruencia sistemática conducen a la necesidad de establecer algún tipo de diferenciación entre las acciones de apoderarse y acceder, previstas conjuntamente en el apartado 2 del artículo 197[95]. Igualmente, desde esta perspectiva, aseverar que la lectura unitaria de todas las acciones elimina la incoherencia de que a conductas de distinto desvalor se le atribuya igual punición no me parece una razón lo suficientemente importante como para desfigurar los elementos de la descripción típica, sino más bien, en todo caso, para exigir la modificación y corrección de las deficiencias de ésta[96]. A este efecto, por supuesto que, en mi opinión, también resulta criticable el hecho de que la consumación se anticipe a la mera puesta en peligro del bien jurídico, motivo por el cual consideraría más acertado ultratraer la intervención penal al momento en que la lesión de éste se produce a través del descubrimiento[97].

---

[93] Consideran que se trata de un delito mutilados de dos actos: RUIZ MARCO, 1999: 55. MORALES PRATS, 2011: 456. JAREÑO LEAL, 2008: 25. ROMEO CASABONA, 2004b: 100, RUEDA MARTÍN, 2004: 51, 81-82.

[94] ROMEO CASABONA, 2004b: 100.

[95] GONZÁLEZ RUS, 2011: 315.

[96] ROMEO CASABONA, 2004b: 115.

[97] RUIZ MARCO, 1999: 154-155.

Las consideraciones expuestas permiten también ofrecer solución a un conjunto de supuestos conflictivos:

a) Contenido inaccesible: Unos pocos autores han discutido acerca de si se puede considerar consumado el delito si el contenido apoderado resulta finalmente inaccesible para el sujeto activo. A mi juicio, debido a que el apoderamiento conduce a la consumación, siendo la intención de descubrir un mero elemento subjetivo que informa la conducta, ambos concurren aunque finalmente la conducta sea inidónea, por lo que se debe apreciar el grado de consumación[98].

b) Disponibilidad momentánea: la misma opinión merece y por las mismas razones el caso en el que el sujeto dispone materialmente del objeto y, posteriormente, habiéndolo examinado y habiendo tomado conocimiento de su contenido, lo vuelve a depositar donde se encontraba[99].

c) Soporte vacío: Un último supuesto sería plantear qué ocurre en aquellos casos en los que el sujeto se apodera de un objeto con ánimo de descubrir la intimidad pero finalmente en el mismo no se contiene ninguna información relativa a la misma. Como señala ANARTE BORRALLO estaríamos ante un supuesto de tentativa absolutamente inidónea, sería impune, como señala el autor, en el que no existe ofensa para el bien jurídico ya que el soporte apoderado no contiene datos íntimos[100].

---

[98] MATA Y MARTÍN, 2001: 129. Consideran que será tentativa DE LA MATA BARRANCO, 2007: 63. DE LA MATA BARRANCO y HERNÁNDEZ DÍAZ, 2010: 176. Igualmente consumado, ORTS BERENGUER y ROIG TORRES, 2001: 31. CARBONELL MATEU y GONZÁLEZ CUSSAC, 2010: CD pág. 1-2.

[99] En sentido similar, plantea GONZALEZ RUS que el apoderamiento no resulta equivalente en este precepto al propio de los delitos contra el patrimonio porque no se pretende la apropiación del objeto, sino que se toma para descubrir un secreto, aunque la tenencia se mantenga sólo unos instantes y luego se devuelva; de hecho si se produce la apropiación efectiva del soporte habrá de apreciarse el correspondiente concurso de delitos con el hurto y el robo. GONZÁLEZ RUS, 2005: 348.

[100] ANARTE BORRALLO, 2001: 53.

B) CONCEPTO DE ACCESO

Establecido desde un punto de vista personal qué debe entenderse por apoderamiento en el seno del artículo 197 y, concluido que apoderamiento y acceso no son conceptos sinónimos, conviene aclarar ahora el término acceso en este mismo precepto. Antes que nada, conviene poner de relieve que, a diferencia del anterior, el verbo acceder es utilizado únicamente en el apartado 2 del artículo 197.

Por lo que respecta a su definición, ésta tampoco está exenta de conflicto. El principal punto de debate se centra en el grado de conocimiento que el sujeto activo debe haber adquirido sobre los datos a los efectos de la consumación del delito, es decir, si meramente debe lograr situarse solo en disposición de conocer el contenido de los datos íntimos[101] o si efectivamente ha de adquirir conocimiento sobre ellos[102]. A continuación se presenta con más detenimiento los argumentos de una y otra postura:

1. ACCESO COMO SINÓNIMO DE ALCANZAR

De acuerdo con un primer grupo de autores, el acceso equivale meramente a conseguir un contacto directo con los datos íntimos. Por consiguiente, según este criterio no sería necesario que el sujeto llegase a conocer o, si se prefiere, a descubrir la información. En esta línea, se ha indicado también que, en función del objeto, acceder supone alcanzar, aunque no obtener o hacerse con el objeto[103].

A favor de esta teoría juegan, en mi opinión, dos argumentos:

---

[101] Parece de esta opinión FERNÁNDEZ TERUELO, 2007:. MORALES PRATS, 2011: 471. ROMEO CASABONA, 2004b: 121. ROMEO CASABONA, 2004a: 198. ROMEO CASABONA, 2004a: 198. RUEDA MARTÍN, 2004: 80.

[102] DOVAL PAÍS, 2000: 104. GONZÁLEZ RUS, 2011: 318. JORGE BARREIRO, 1997: 574. JORGE BARREIRO, 2002: 119. JORGE BARREIRO, 2011: 868. ORTS BERENGUER y ROIG TORRES, 2001: 31, 35. QUERALT JIMÉNEZ, 2010: 299.

[103] ANARTE BORRALLO y DOVAL PAÍS, 2012: 19.

a) Teoría de la espiritualización del concepto de apoderamiento: cabe recordar que los partidarios de esta teoría concebían como conceptos sinónimos los verbos acceder y apoderarse (de hecho el primero se utilizaba para definir el segundo), y luego entendían que para la consumación del delito no era necesario el descubrimiento o la obtención de conocimiento sobre los datos, que actuaba meramente como un elemento subjetivo del injusto[104].

b) Los ficheros como objeto material del delito: en el apartado 2 se sancionan un conjunto de acciones cuya tortuosa redacción ha impedido a la doctrina llegar a cualquier tipo de acuerdo sobre la interpretación de su entramado típico, habiéndose llegado incluso a afirmar que no es posible encontrar *razón alguna capaz de explicar las diferencias entre el inciso inicial y el final*[105]. Estas conductas se dividen, específicamente, en dos incisos: por una parte, el apoderamiento, la utilización y la modificación de datos reservados de carácter personal o familiar de otro que se hallen registrados en ficheros o registros; por otra, el acceso la alteración o utilización de los mismos[106]. Pues bien, la cuestión debatida al respecto es si la expresión *a los mismos* del segundo inciso tiene como objeto material del delito a los datos o a los ficheros. A los efectos de intentar dar respuesta a esta cuestión se han planteado dos tesis, cada una de las cuales tiene sus ventajas e inconvenientes. Son las que se presentan a continuación:

---

[104] Véase Epígrafe anterior.

[105] GONZÁLEZ RUS, 2011: 319.

[106] *Las mismas penas se impondrán 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.*

aa) Los ficheros o registros como objeto material: unos pocos autores defienden una corriente iniciada por CARBONELL MATEU y GONZÁLEZ CUSSAC , quienes vinculan dicha expresión a los ficheros o registros y no a los datos, al entender que, en caso contrario, el inciso segundo estaría reiterando dos de las tres conductas previstas en el inciso primero —utilización y alteración, considerando equivalentes los términos alteración y modificación—, produciéndose una superposición carente de sentido entre los dos incisos[107].

bb) Los datos como objeto material del delito: que, precisamente se trata de una superposición entre ambos incisos y que el objeto material de ambos son los datos es lo que defiende la postura mayoritaria[108].

---

[107] Con razón matiza RUIZ MARCO que, pese a lo fundado de las críticas que se realizan al mismo, no parece encontrase otra exégesis que justifique la vigencia y funcionalidad del párrafo en cuestión. CARBONELL MATEU y GONZÁLEZ CUSSAC, 2010: 1 CD. CASTIÑEIRA PALOU, 2010: 147. QUERALT JIMÉNEZ, 2010: 299. RUIZ MARCO, 2001: 78.

[108] La conclusión lógica de esta postura es que ambos incisos castigan idénticas conductas y que el segundo no supone más que una reiteración superflua y vacía de contenido. Efectivamente, un sector mayoritario rechaza la postura doctrinal expuesta por entender que, a pesar de ser bien intencionada (GONZALEZ RUS) e ingeniosa (ORTS BERENGUER Y ROIG TORRES), es *poco útil* (GONZALEZ RUS) *insostenible* (JORGE BARREIRO), por ser una *interpretación tan forzada que acaba incurriendo en otros contrasentidos* (MORÓN LERMA) y que *tiene un coste muy alto* (MORALES PRATS) debido a las *incongruencias sistemáticas* que origina (RUIZ MARCO). Los argumentos que se han aducido al respecto son: que centra el objeto material en el continente en lugar del contenido (RUIZ MARCO), lo que provoca un desenfoque teleológico desde la perspectiva del bien jurídico protegido (MORALES PRATS, JORGE BARREIRO), al suponer un adelantamiento excesivo de la tutela penal que no está justificado político-criminalmente (MORALES PRATS) y al contradecir la letra de la ley (JORGE BARREIRO), y ocasiona penológicamente la incongruencia de castigar una conducta con lesividad menor (la relativa a los ficheros) con la misma pena que los comportamientos dirigidos contra los datos (ORTS BERENQUER y ROIG TORRES) DE LA MATA BARRANCO y HERNÁNDEZ DÍAZ, 2010: 175. GONZÁLEZ RUS, 2011: 318. JORGE BARREIRO, 1997: 574. JORGE BARREIRO, 2002: 117. LOZANO MIRALLES, 1998a: 216. MORALES PRATS, 2011: 471. MORÓN LERMA, 2002a: 62. MUÑOZ CONDE, 2015: 237. ORTS BERENGUER y ROIG TORRES, 2001: 34. REBOLLO VARGAS, 2004: 467. RUIZ MARCO, 2001: 78. TOMÁS - VALIENTE LANUZA, 2010: 801. A esta postura se adhiere también la jurisprudencia: SAP Barcelona 6ª 219/2006, de 1 de marzo y STS de 8 febrero de 1999

La aceptación de la primera postura, la cual, desde luego, me parece la más coherente con el tenor literal del artículo 197.2[109], me conduce a situar la consumación del delito en el momento en que tiene lugar la apertura del fichero o registro, lo que impide entender que se haya adquirido conocimiento sobre cualquier dato en ellos contenido. Es por ello que, admitiéndose esta postura, queda absolutamente patente que acceder no supone adquirir conocimiento de los datos, pues el sujeto estaría meramente en disposición de conocer y obtener los datos reservados de carácter personal y ello sería suficiente para consumar el tipo penal.

---

[109] De las dos opiniones expuestas, por tanto, la primera es la que me parece más coherente con la descripción típica, motivo por el cual no comparto ninguna de las críticas realizadas debido a los siguientes motivos:

a) Mientras el conocimiento de los datos supondría la lesión de la intimidad, el acceso al fichero implicaría como mínimo la puesta de peligro de ésta.

b) Además, la previsión de idéntica pena para conductas con diferente desvalor es un argumento que no puede justificar que ello no suceda en el Código penal, pues es ya el propio apartado 1 del artículo 197 el que sanciona con igual pena conductas de diferente desvalor. Así pues, en palabras del propio MORALES PRATS, en este último se *desatiende la diversa insidiosidad que para el bien jurídico suscita el empleo de un mero apoderamiento físico de documentos o efectos personales frente a la utilización de sofisticados aparatos de control auditivo o visual clandestino; estos últimos proporcionan un control certero y sistemático, más penetrante que pasa inadvertido para la víctima, lo que debería haberse visto reflejado en un distinto trato punitivo más grave para estos últimos casos. Una estratificación de las penas hubiera sido aconsejable desde el punto de vista del principio de proporcionalidad.*

c) Sí es cierto que desde una perspectiva de los principios de *ultima ratio* y fragmentariedad del Derecho penal, no me parece político-criminalmente adecuado adelantar tanto la barrera punitiva, pero ello es característica ínsita al proceso de expansión del Derecho penal que, se quiera o no, es una realidad.

d) Desde un punto de vista gramatical, la referencia a los mismos puede ser dirigida tanto a los datos como a los ficheros, pues nada aclara la letra de la Ley en uno u otro sentido.

Por todo ello, debo concluir junto a RUIZ MARCO que, si bien el apartado, al igual que su predecesor sistemático, es susceptible de numerosas y fundadas críticas, no parece posible conforme a la redacción vigente interpretación distinta a la ofrecida. MORALES PRATS, 2011: 454, 472. ORTS BERENGUER y ROIG TORRES, 2001: 34. REBOLLO VARGAS, 2004: 456. RUIZ MARCO, 2001: 78.

2. ACCEDER COMO SINÓNIMO DE CONOCER

Otro grupo de autores, minoritario, se manifiesta a favor de una mayor restricción del injusto típico y considera que acceder equivale a conocer[110]. Así, definen el acceso como conocimiento u obtención de información sobre los datos personales registrados[111], aunque, en ocasiones, también se hace referencia a *tenerlos a disposición*[112] o *hacerlos propios*[113].

Desde esta perspectiva, algunos autores puntualizan que el término conocimiento tampoco puede ser interpretado en sentido amplio, como simple conocimiento de datos, pues ello podría conducir a un injustificado alargamiento de la cadena delictiva hasta el infinito, es decir, a todos aquellos sujetos que fueran tomando conocimiento sucesivamente de la información sin haber accedido directamente a ella sino por referencia de otro sujeto[114]. Es por ello que consideran que debe exigirse para la relevancia típica de la conducta, al menos un contacto directo con el continente del dato[115], en concreto, una acción mediante la cual se supere alguna barrera, aunque sea mínima, de resguardo de los datos[116].

---

[110] En relación con el apartado 2 del artículo 197, este sector de la doctrina exige una mínima captación mental del contenido, no sólo la mera visión o la apertura del documento que contiene los datos, pero sin que exista la aprehensión física o la reproducción de los mismos. GONZÁLEZ RUS, 2011: 319.

[111] JORGE BARREIRO, 2011: 868 párrafo 9900.

[112] JORGE BARREIRO, 2011: 868 párrafo 9900.

[113] GONZÁLEZ RUS, 2011: 318.

[114] DOVAL PAÍS y JAREÑO LEAL, 2000: 3. DOVAL PAÍS, 2000: 104. ORTS BERENGUER y ROIG TORRES, 2001: 35. JORGE BARREIRO, 2002: 119.

[115] JORGE BARREIRO, 2002: 119.

[116] Para JAREÑO LEAL y DOVAL PAIS, el acceso, para ser típico, requiere el contacto directo entre quien accede y la instalación o soporte informático que contiene los datos. Para ellos, en el contexto del tipo, acceso no equivale a conocer, saber o enterarse, sino a entrar (o tener paso), en sentido figurado, en la instalación informática como forma de enterarse de los datos personales. DOVAL PAÍS, 2000: 104. DOVAL PAÍS y JAREÑO LEAL, 2000: 3. DOVAL PAÍS y JAREÑO LEAL, 2001: 1484-1485.

3. TOMA DE POSTURA

Me inclino por la primera postura con base a un único argumento: el objeto material del delito son los ficheros y los registros informáticos. Resultaría incongruente, por tanto, hacer referencia a conocimiento de datos si éstos no son el objeto material del delito, de modo que, a mi juicio, CARBONELL MATEU y GONZALEZ CUSSAC es la opción más adecuada y, además, no me parece posible conforme a la redacción vigente mantener una interpretación distinta a la ofrecida.

Es cierto que, al igual que sucede en el apartado 1, se produce la punición de conductas de distinto desvalor a través de las mismas penas, pero me parece aun peor —y totalmente desaconsejables desde la perspectiva del principio de vigencia— dejar vacío de contenido todo un inciso completo del Código penal, más cuando desde el punto de vista del principio de legalidad, ambas interpretaciones son posibles. Efectivamente, la norma legal no prohíbe dicha interpretación y mientras no se derogue el precepto deberá buscarse la interpretación más acorde con el tenor de la Ley, que en este caso resulta ser la realizada por CARBONELL MATEU y GONZÁLEZ CUSSAC.

Desde una perspectiva del respeto al principio de *ultima ratio* me parece excesiva la punición del acceso a ficheros o registros de datos, que castigan meramente el peligro que hipotéticamente pudiera derivarse en un momento posterior una lesión de la intimidad. La intervención penal debiera reservarse para los ataques más importantes a los bienes más importantes y creo que esta conducta no ofrece la ofensividad al bien jurídico necesaria para mantenerse en el Código penal. Aun así, si el legislador deseara mantenerla, lo adecuado (y lo más ajustado a la proporcionalidad) sería preverla como un tipo privilegiado respecto de las anteriores, pero no como un tipo mixto alternativo.

Reflejo sino directo bastante claro de la disyuntiva presentada en las páginas anteriores en relación con la interpretación de ambas modalidades lo constituye la Sección 202a del Código penal alemán. Ésta recoge el delito de *Ausspähen von Daten* o espionaje de datos, que castiga a quien se procure para sí o para un tercero acceso datos que no estén destinados para él y que hayan sido especialmente asegurados contra su acceso no autorizado a través de la superación de las medidas de seguridad[117].

Al amparo de esta redacción distingue desde 2007[118] la doctrina la doctrina dos acciones: procurarse datos (*Verschaffen von Daten*) y procurarse el acceso a los datos (*Verschaffen des Zugangs zu Daten*)[119]. Como se verá, trasladando esta idea al artículo 197.1 y .2 del Código penal español, mientras que la primera modalidad se correspondería con la conducta de apoderamiento, la segunda se correspondería con la modalidad relativa al apartado .2 y, más concretamente, con la redacción que el artículo 197.3 tenía entre los años 2010 y 2015. De esta manera, la interpretación de este precepto del Código penal alemán sirve como medio de corroborar la diversidad material de ambas acciones.

Aunque el legislador alemán no ha ofrecido una definición de lo que debe entenderse por procurarse (*verschaffen*), la doctrina alemana define de un modo genérico esta acción como el acto de proporcionarse para sí o para un tercero datos informáticos o un soporte que contenga tales datos[120]. Ello puede tener lugar, como he dicho, a través de las siguientes modalidades:

---

[117] *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*

[118] Véase Capítulo II.

[119] GRAF, 2012: 196 párrafo 49.

[120] ALTENHAIN y WIETZ, 2013b: 1590.

a) ***Verschaffen von daten*** **(apoderamiento de datos):** El control sobre los datos implica la efectiva adquisición por parte del sujeto activo de la posesión sobre los datos, lo que puede tener lugar de dos formas: o bien mediante la obtención material de los datos a través de obtención del dispositivo original de almacenamiento donde éstos se encuentran, la realización de una copia de los datos mediante una máquina fotocopiadora, el traslado a otro dispositivo de almacenamiento, su impresión, grabación o filmación, o a través de cualquier otra forma que permita obtenerlos de forma física; o bien mediante su obtención inmaterial a través de la obtención del conocimiento directo sobre los mismos, lo que permite al sujeto retenerlos mentalmente en su cabeza o escribirlos[121]. La consumación de esta modalidad se produce cuando el autor o el tercero consigue obtener un verdadero control sobre los datos[122]. Se observa, pues, en esta primera modalidad una interpretación vinculada al sentido apuntado para la acción de apoderamiento: apropiación de los datos o el soporte, poder de disposición sobre éstos, con independencia de su conocimiento efectivo.

---

[121] La opinión de los autores en relación con la admisión de una u otra forma de apropiación no es unánime. Se citan como ejemplo de esta conducta se encuentran el fotocopiado, fotografiado o grabación en video de los datos, así como la realización de una captura de pantalla del monitor o su impresión. Se excluye, sin embargo, la apropiación de un papel impreso o la mera instalación de un programa. Igualmente, se excluye de este supuesto el acceso inicialmente autorizado, pero con apoderamiento ulterior en tanto extralimitación del acceso lícito *ab initio*. GRAF, 2012: 196 párrafo 49; 197 párrafo 52. KARGL, 2013b: 1413 párrafo 12. WEIDEMANN, 2010: 1309 párrafo 15.

[122] Dentro del tipo penal se prevé un esquema doble: por una parte, la posibilidad de que el autor directo del delito se procure para sí los datos, caso en el que sería él mismo a quien se le exigiera para la perfección del delito la obtención de un poder de disposición para entender perfeccionado el delito; por otra parte, es posible que el autor directo sólo consiga el soporte o los datos con la finalidad de entregárselo a un tercero, siendo que éste será quien obtiene el control sobre los datos o su conocimiento, manteniéndose la autoría del delito en el sujeto anterior. BOSCH, 2014: 1277 párrafo 6. GRAF, 2012: 197 párrafo 54. KARGL, 2013b: 1413 párrafo 12. KINDHÄUSER, 2013: 746 párrafo 5. HEGER, 2014: 922 párrafo 5.

b) ***Verschaffen des zugangs zu daten*** **(acceso a datos):** Esta conducta se define como la acción de penetrar mediante superación de las medidas de seguridad en un dispositivo de almacenamiento de datos, un ordenador, una red o la línea a los efectos de conseguir una situación en la que el autor o un tercero se encuentre en la posibilidad de percibir el contenido del sistema informático o copiarlo[123]. La consumación del delito se produce cuando el sujeto ha superado las medidas de seguridad dispuestas para impedir el acceso a los datos informáticos, hecho que le otorga un contacto directo, esto es, un poder de disposición sobre los datos[124]. La disponibilidad sobre los datos se puede obtener bien mediante la superación de las medidas de seguridad o también mediante la averiguación subrepticia de las claves o datos que permiten lograr el acceso a tales datos[125]. Sin embargo, no es sea necesaria la obtención del contenido del soporte o la toma de conocimiento sobre el mismo[126]. Como se observa, la conducta de acceso es una conducta inmaterial, en la que no se produce la adquisición de un poder de disposición sobre los datos y, en la que únicamente se suscita la necesidad o no de exigir para su consumación el conocimiento de los mismos.

---

[123] ALTENHAIN y WIETZ, 2013b: 1590 párrafo 7.

[124] BOSCH, 2014: 1277 párrafo 6.

[125] GRAF, 2012: 197 párrafo 53. KARGL, 2013b: 1413 párrafo 12.

[126] BOSCH, 2014: 1277 párrafo 6.

SUBSECCIÓN 2ª

LA ACCIÓN DE ACCEDER EN EL ARTÍCULO 197.1 BIS

I. LA ACCIÓN DE ACCESO EN EL SENO DEL ARTÍCULO 197.1 *BIS: ANÁLISIS COMPARADO*

Hasta el momento se ha analizado la acción de acceder en el artículo 197.2 del Código penal español, el cual, como se ha visto, toma como objeto material los datos. La referencia a éstos ha constituido, en consecuencia, el punto de partida de la definición de acceso presentada en el capitulo anterior, hecho que encajaba perfectamente con la derogada regulación que introdujo el acceso ilícito como un tipo de equivalencia con el delito de descubrimiento y revelación de secretos en el que el objeto material eran también los datos.

Sin embargo, de acuerdo con la nueva redacción de la conducta ofrecida por la Ley Orgánica 1/2015, el acceso se ha desvinculado de los datos y programas informáticos para, a mi juicio acertadamente, adoptar como objeto material del delito el sistema informático. Se centra, pues, la atención en el continente y no en el contenido.

Su examen exige, por tanto, ampliar los márgenes de estudio para prestar atención a la regulación que de ella han hecho otros países con mayor tradición en la materia, lo que permitirá, sin perder de vista la sistematización de nuestro Código penal, ya apuntada en el capítulo anterior, fijar su alcance y contenido prestando atención al nuevo objeto material del delito: el sistema informático.

A) CONCEPTO DE ACCESO

La primera cuestión que se resaltaba respecto de la definición de acceso y apoderamiento en el seno del artículo 197 era la falta de una definición unánime en la doctrina. Lo mismo sucede en este punto. Así pues, son múltiples las definiciones que la doctrina de los distintos países ha ofrecido con el objetivo de delimitar el acceso. Nuevamente, pueden observarse las dos posturas que se han comentado en relación con el apartado 2 de dicho precepto.

1. ACCESO COMO SINÓNIMO DE PENETRAR

La primera postura considera acceder como sinónimo de penetrar o introducirse en el sistema[127]. Desde esta perspectiva, algunos autores ponen el acento en el continente, esto es, el propio sistema informático[128], mientras que otros autores ponen el acento en el contenido de éste, los datos informáticos, y lo conceptúan sobre la

---

[127] También CANNATA, 2006: 536.

[128] BORRUSO y también GALDIERI, que definen el acceso abusivo como la efectuación en un sistema informático ajeno de operaciones no consentidas por el titular del sistema. CUOMO afirma que acceso reclama alguna actividad que sea idónea para poner en comunicación un ordenador llamante con un ordenador contestador. MARINI considera que se trata de cualquier forma de intromisión en el sistema informático o telemático no abierto o cuyo acceso sea reservado o garantizado mediante la utilización de una clave de acceso (no todas las medidas de seguridad son contraseñas). PICA entiende que introducirse en el sistema informático consiste en acceder al interior del sistema, utilizando su propia tecnología. A ello añade que la generalidad del término introducirse deja espacio a cualquier tipo de conducta que permita al sujeto activo introducirse, pero en todo caso esto supondrá la realización de actos físicos dirigidos al acercamiento al sistema, unidos a una introducción electrónica que tiene lugar con la utilización del hardware, del software así como de los programas que consienten leer el contenido del sistema y eventualmente actuar en consecuencia. VICARIOLI cualquier tipo de interferencia posibilitada por el desarrollo técnico en el programa o en la memoria de un aparato informático o telemático no abierto y garantizado de una clave de acceso u otro medio de protección, en contra de la voluntad del titular del *ius excludendi*. BORRUSO, 1994b: 32. CUOMO y RAZZANTE, 2009: 96. GALDIERI, 1996: 48. MARANI, 2007: 618. VICARIOLI, 2008: 246.

base de cómo se articula la conducta respecto de éstos[129], si bien algunos autores utilizan ambos[130].

2. ACCESO COMO CONOCIMIENTO DE DATOS[131]

Un segundo grupo de autores muy minoritario se manifiesta a favor de una mayor restricción del injusto típico y considera que acceder equivale a conocer y, así, definen el acceso como conocimiento, al considerar que la mera introducción en sí misma no parece merecedora de criminalización[132].

---

[129] ALTENHAIN: penetrar en el dispositivo de almacenamiento de datos, ordenador, red o la línea. CECACCI, que considera acceso como la operación a través de la cual el sujeto activo puede introducirse en un sistema informático a fin de obtener la disponibilidad de un determinado dato registrado en un archivo electrónico y, a su vez, distingue acceso de introducción abusiva, esto es, la inserción o acceso a los archivos (informaciones y datos) sin el consentimiento de la parte interesada o en los programas contenidos en la memoria del sistema contra la voluntad de quien tiene el derecho a vetarlo. PECORELLA lo concibe como obtener acceso a la memoria interna del sistema, introduciéndose en la condición de poder obtener datos y programas que están registrados o que están eventualmente contenidos en soportes externos del sistema que están conectados con él. CECCACCI, 1994: 71, PECORELLA, 2006: 335, ALTENHAIN y WIETZ, 2013b: 1590 párrafo 7.

[130] PARODI debe entenderse como tal no tanto el contacto físico cuanto el lógico, esto es la superación de los medios de protección del sistema y el inicio del diálogo con el mismo de tal forma que el agente se encuentra en la condición de conocer directamente datos, informaciones y programas. PARODI y CALICE, 2001: 64-66.

[131] ATERNO, 2000: 2990. CECCACCI, 1994: 71. LATTANZI y LUPO, 2010: 1357.

[132] MANTOVANI define la conducta como acceder al conocimiento de datos o informaciones contenidas en el sistema, mediante la inmisión en el mismo a través de operaciones o dispositivos técnicos dirigidos a tal propósito. Para el autor no caen dentro del ámbito del precepto la toma de conocimiento del contenido del sistema sin previo acceso al mismo, como tiene lugar en aquellos casos en los que se produce la mera lectura de datos o información impresos o mostrados en el monitor. TRENTACAPILLI afirma que introducirse va más allá del mero acceso y que el resultado de la acción supone el conocimiento de las noticias y la información confidencial contenida en el sistema. BASSANI, afirma que el acceso abusivo al sistema puede consistir tanto en la mera lectura de datos contenidos en el sistema, a través de la lectura de la pantalla, como en la copia de los mismos. KARAGIANNOUPOULOS lo define como la acción del outsider que no tiene autorización para acceder a un determinada red de ordenadores así como a la información contenida en ella, consiguiendo traspasar los controles técnicos que previenen a los usuarios no autorizados el acceso y el uso de la información o de los recursos informáticos. MANTOVANI, 2011: 543. TRENTACAPILLI, 2002: 1283. KARAGIANNOPOULOS, 2014: 466.

3. VALORACIÓN PERSONAL

En mi opinión esta **acción**, a la que coloquialmente se hace referencia como hackear[133], implica una intrusión de carácter electrónico por parte del sujeto activo en un sistema informático ajeno[134] a través de la realización en el mismo de operaciones no consentidas por el titular[135].

Muy acertadamente algunos autores afirman que se trata de una **introducción electrónica** en el sistema[136], ya que para culminar dicha injerencia en el sistema ajeno resulta indispensable no sólo el mero contacto con el hardware del sistema, sino también la iniciación de un diálogo activo con el software, siendo esto último —el diálogo con el software— el elemento fundamental e indefectible que permite concluir la efectiva realización del acceso[137]. El hecho de que el objeto material protegido sea el continente y no el contenido conduce a excluir cualquier tipo de toma de conocimiento sobre los datos como elemento del tipo. Cuestión distinta es la de que, como muy acertadamente plantea la doctrina, se contemple también a éste en la definición del primero. Sin embargo, acceder excluye de todo punto la obtención del control sobre los datos en el sentido que exige el apoderamiento. Acceder al sistema implica **mera introducción sin posesión y sin conocimiento**.

---

133 ALTENHAIN y WIETZ, 2013a: 1590. JOECKS, 2010: rn 10 pág. 352.

134 La utilización del verbo introducirse en la definición de la acción de acceso es completamente deliberada. La razón de esta elección sobre cualquier otro término se debe a que éste es el verbo empleado en la descripción de este comportamiento típico en el artículo 615 *ter* del Código penal italiano. En este sentido, en dicho país es unánimemente admitido que ambos conceptos, introducción y acceso, son sinónimos ya que, de hecho, el motivo por el cual se ha usado específicamente en la redacción del delito el termino introducirse en lugar de acceder se halla en la propia incriminación de la conducta como un tipo de equivalencia con el delito contra la inviolabilidad del domicilio, donde ésta es característica. CANNATA, 2006: 536. PECORELLA, 2006: 333. PICA, 1999: 40.

135 BT-Drucksache 16/3656, 2006: 9. CADOPPI et al., 2011: 535. PICA, 1999: 41. CANNATA, 2006: 536.

136 BORRUSO et al., 1994: 32. CECCACCI, 1994: 71. CUOMO y RAZZANTE, 2009: 96. GALDIERI, 1996: 48. MARANI, 2007: 618. PECORELLA, 2006: 335. PICA, 1999: 41/56. PARODI, 2000: 653.

137 CADOPPI et al., 2011: 535. RELLA, 2007: 43. PARODI, 2000: 653. MAIORANO, 2010: 1357.

B) TIPOS DE ACCESO

1. ACCESO FÍSICO VS. ACCESO REMOTO

Desde un punto de vista fáctico, la Ley permite dar una cobertura igualitaria y global a todos los posibles ataques contra el bien jurídico protegido, esto es, tanto a los ataques de tipo físico como a aquellos que se producen de forma remota[138].

> **a) Acceso físico o directo:** supone la intervención física, directa o material del sistema informático por parte del sujeto activo, que se introduce en él desde el mismo lugar donde se encuentra utilizando únicamente sus propios elementos de hardware y software.
>
> **b) Acceso lógico o remoto:** consiste en la introducción indirecta o virtual en el sistema informático accedido, utilizando otro sistema informático o cualquier otro dispositivo electrónico o telemático que, mediante software, permita el intercambio de información para introducirse en el sistema informático objeto de acceso, lo que exige que ambos sistemas estén conectados o bien a una red de área global como Internet o bien a una red de área local.

La admisión de ambas formas resulta controvertida en la doctrina comparada. De este modo, mientras un sector se muestra favorable a entender englobados ambos tipos de acceso[139], otro sector considera esta última forma de acceso, la remota, el único procedimiento posible de comisión de este delito y niega, por tanto, que el acceso físico pueda considerarse típico[140], reconduciendo su punición a otros tipos como el allanamiento de morada[141].

---

[138] D'AIETTI, 1994a: 69. GAROFOLI, 2013: 643. PECORELLA, 2006: 359. Igualmente en Francia se admiten ambos tipos de acceso (véase la Sentencia de la Corte de Apelación de París de 5 de abril de 1994)

[139] DESTITO et al., 2007: 84 nota 9. DELPINO, 2003: 585. DOLCINI y MARINUCCI, 2011: 5985. GALDIERI, 2001: 81. DI GIANNANTONIO, 1997: 435. PICA, 1999: 42. GRAF, 2012: rn. 33.

[140] D'AIETTI, 1994b: 68-69. CUOMO y RAZZANTE, 2009: 97. MAIORANO, 2010: 1357. PARODI, 2000: 653. PICA, 1999: 41. FIANDANCA y MUSCO, 2013: 293. TRENTACAPILLI, 2002: 1283. MARANI, 2007: 618. PARODI y CALICE, 2001: 64, 67.

[141] Sobre el particular, véase Capítulo VI.

Las razones que alegan para excluir de la tipicidad el acceso físico los autores que se decantan por esta última postura son las siguientes:

a) Contacto electrónico: teniendo en cuenta que el acceso exige una introducción de carácter electrónico en un sistema informático ajeno, el sujeto activo deberá en cualquier caso hacer uso de un sistema informático para poder cometer el delito. Por este motivo, algunos autores consideran que el tipo penal solo puede castigar el acceso remoto, ya que ésta es la única forma de intromisión idónea para generar el diálogo exigido para crear la comunicación con el sistema informático[142].

b) Afectación del bien jurídico: en tanto en cuanto solo se considera acceso una introducción electrónica en un sistema ajeno, este sector de la doctrina considera que esta es la única vía a través de la cual se puede producir el menoscabo del bien jurídico tutelado en el delito[143].

c) Necesaria restricción del ámbito aplicativo del precepto: en tanto que, como se ha dicho, el acceso requiere una conexión electrónica con el sistema y que, además, la perfección del delito exige en todo caso la superación de las medidas de seguridad dispuestas para impedir el acceso, resulta adecuado al principio de ofensividad para este sector restringir el ámbito aplicativo del precepto únicamente a la a la modalidad de acceso de carácter remoto. La principal razón de lo anterior estriba en que tan solo cuando el sujeto activo ha vulnerado las medidas lógicas se encuentra en la condición de conocer directamente datos, informaciones o programas en él contenidos[144].

---

[142] CUOMO y RAZZANTE, 2009: 97.

[143] FIANDANCA y MUSCO, 2013: 293. MARANI, 2007: 618.

[144] PARODI y CALICE, 2001: 64.

2. ACCESO TOTAL VS. ACCESO PARCIAL[145]

Desde esta perspectiva el Código parece distinguir entre el **acceso parcial y acceso total** al sistema informático. Aunque desde un punto de vista descriptivo resulta muy fácil entender dicha frase, la interpretación de este apartado puede resultar *a priori* conflictiva especialmente por lo que se refiere acceso a la totalidad del sistema. Así pues, podría considerarse que el tenor literal del precepto se está refiriendo a acceder a la totalidad del contenido del sistema, lo que no concordaría en ningún caso con el perfil jurídico-interpretativo que se ha presentado en el presente estudio, alteraría el momento de consumación del delito adelantándolo al inicio del contacto con el sistema.

Sin embargo, no debe considerarse la inclusión de este inciso como una incongruencia, sino que, en mi opinión, esta "coletilla" lo que hace es contribuir a determinar el momento consumativo. Así pues, como se verá en el siguiente epígrafe[146], en el momento en que se tenga disponibilidad de la totalidad del sistema se habrá consumado el delito, pero en aquellos casos en los que se tenga disponibilidad sobre una parte del sistema existiendo una parte especialmente protegida sobre la que no se adquiera disponibilidad, entonces se tratará de un acceso parcial, consumándose la conducta igualmente por estar en condiciones el sujeto de acceder al contenido de la parte que ha logrado desproteger. Éste es, pues, el sentido que creo debe dársele a esta cláusula del tipo.

---

[145] Una crítica similar podría realizarse a la redacción de la conducta entre 2010 y 2015, la cual exigía que los datos y programas accedidos debían contenerse en todo o en parte del sistema. Con la redacción del apartado 3 del artículo 197 tal y como fue redactado por la reforma operada por la Ley Orgánica 1/2010, de 22 de junio, el alcance de la conducta de acceso adolecía de una falta de claridad tal que vagaba entre la incongruencia y la incoherencia. Son dos las críticas que podían realizarse a la redacción hoy derogada: a) Falta de fidelidad al texto originario. b) Incongruencia descriptiva.

[146] Para un análisis más detallado véase el próximo apartado C) CONSUMACIÓN Y TENTATIVA

C) CONSUMACIÓN Y TENTATIVA

De la propia configuración del concepto de acceso, dependerá la determinación del momento exacto en el que se produce la consumación del delito y la delimitación del ámbito de la tentativa. Al respecto hay que recordar que tanto 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[147], como el Convenio sobre la Ciberdelincuencia, hecho en Budapest el 23 de noviembre de 2001, contienen disposiciones específicas para la regulación de la tentativa[148]; no obstante, ninguna de ellas afecta al artículo 2, que es el relativo al acceso ilícito.

En cualquier caso, en España se castiga la tentativa del delito, como se verá[149], mediante un sistema de regulación abierto en la parte general del Código penal. Lo anterior se diferencia, por tanto, del sistema de incriminación seguido en otros algunos países, cuyos sistemas penales contemplan este instituto a través de decisiones singulares, en función de cada tipología delictiva, diferenciando la incriminación de las formas de tentativa de forma separada[150].

---

147 Artículo 8 Inducción, complicidad y tentativa

2. *Los Estados miembros garantizarán que la tentativa de cometer las infracciones mencionadas en los artículos 4 y 5 sea sancionable como infracción penal.*

148 Article 11 – Attempt and aiding or abetting.

2. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, an attempt to commit any of the offences established in accordance with Articles 3 through 5, 7, 8, and 9.1.a and c of this Convention.

3. Each Party may reserve the right not to apply, in whole or in part, paragraph 2 of this article.

149 Al análisis de la tentativa se dedica el apartado 2. del presente epígrafe.

150 Señalan también el carácter abierto del sistema de punición de la tentativa en EspañaANARTE BORRALLO y DOVAL PAÍS, 2012: 30.

1. CONSUMACIÓN

En la doctrina comparada existen tres posturas completamente diferenciadas sobre el momento en que ésta tiene lugar. Para explicarlas, en aras a ofrecer un mayor entendimiento de cada uno de los grupos de propuestas que se presentarán, voy a explicar brevemente como se articula desde un punto de vista fenomenológico dicho delito. El procedimiento que seguirá el autor para acceder al sistema ajeno puede dividirse en dos fases[151]:

> **a) Contacto con el sistema:** por una parte, caracteriza el acceso una fase de carácter físico, que estaría integrada por la mera conexión o interacción del sujeto con el hardware del sistema accedido.
>
> **b) Introducción electrónica:** Una vez finalizada dicha conexión, se inicia la segunda fase, que implica la efectiva consecución de un diálogo con el software del sistema accedido.

a) POSTURA AMPLIA: CONTACTO CON EL SISTEMA

Una primera postura, más amplia y, a la vez, la minoritaria[152], considera que la consumación del delito se produce en la primera fase, cuando el sujeto activo realiza el primer contacto con el sistema, o, incluso antes, cuando está en disposición de conocer la clave de acceso al sistema o de desactivar los medios de protección, sin que sea necesario que supere las barreras lógicas o físicas dispuestas para proteger el sistema accedido y, aun menos, que obtenga conocimiento sobre datos informáticos.

---

[151] CADOPPI et al., 2011: 535. PICA, 1999: 40-41. RELLA, 2007: 43.

[152] Estos autores conciben el delito como un tipo de peligro, llegando incluso a considerar que la consumación del delito puede producirse sin poner realmente en peligro al bien jurídico a causa de circunstancias sobrevenidas, situaciones o elementos externos del todo punto independientes de la voluntad del agente. MARANI, 2007: 618. FONDAROLI, 1996: 312. Admiten en Alemania la mera posibilidad de interactuar con el contenido o consideran colmada esta exigencia con la mera averiguación de los datos para sobrepasar las medidas de seguridad, eso es, la posibilidad de descodificar. SCHUHR, 2010: 156. VASSILAKI, 2008: 349.

b) POSTURA INTERMEDIA: SUPERACIÓN DE LAS MEDIDAS

Mayoritariamente se defiende que para la consumación no es suficiente con el simple contacto con el sistema o el mero acceso, sino que se exige un paso más[153]. Ésta postura, intermedia entre la inmediatamente expuesta y la que a continuación explicaré, hace depender la perfección del delito de dos circunstancias: por una parte, de la superación de las medidas de seguridad de las que está dotado el sistema; por otra, de la obtención por parte del sujeto de un poder de disposición sobre el sistema.

La **superación de las medidas de seguridad** tiene lugar tras el traspaso por el sujeto de todos y cada uno de los obstáculos dispuestos por el titular del sistema para impedir el acceso al mismo[154]. El cumplimiento del anterior requisito permite constatar la **disponibilidad del sujeto activo sobre el sistema**, situándose éste ante la posibilidad de interactuar con el contenido, es decir, de acceder a él, conocerlo o copiarlo y produciéndose la perfección el tipo[155].

---

[153] **Doctrina italiana:** ANTOLISEI, 2008: 240. ALIBRANDI, 2011: 1756. BORRUSO, 1994a: 28. CANNATA, 2006: 538. CARINGELLA et al., 2010: 1054.. CECCACCI, 1994: 71. CUOMO y RAZZANTE, 2009: 96. DE SANZO et al., 2009: 898. DELPINO, 2003: 585. DESTITO et al., 2007: 89. PECORELLA, 2011: 5982, 5985, 5987. GAROFOLI, 2013: 644, 648. GATTA, 2011: 300. MAIORANO, 2010: 1357, 1368. MELONI, 2012: 2994. PARODI y CALICE, 2001: 64, 66. PECORELLA, 2006: 335-336. PICA, 1999: 57. FLOR

Doctrina alemana: ALTENHAIN y WIETZ, 2013b: 1590 párrafo 7. GRÖSELING y HÖFINGER, 2007: 551. FISCHER, 2013: 1361 párrafo 10. HILGENDORF, 2005: párrafo 16. BOSCH, 2014: 1277 párrafo 6. GERCKE y BRUNST, 2009: 69 párrafo 97. GRAF, 2012: 191 párrafo 36. HEGER, 2014: 922 párrafo 5. HOYER, 2012: 6 párrafo 11. KARGL, 2013b: 1413 párrafo 14. KINDHÄUSER, 2013: 746 párrafo 5. KRUTISCH, 2004: 123. KUSNIK, 2012: 82. LENCKNER y EISELE, 2010: 1822 párrafo 10. SCHMITZ, 1995: 483. TAG, 2013: 1092 párrafo 8. WEIDEMANN, 2010: 1309 párrafo 15.

[154] Se ha discutido si existe disponibilidad en aquellos supuestos en los que, además de medidas de seguridad dispuestas genéricamente sobre el sistema, los datos contenidos se hallan especialmente protegidos contra su acceso. La respuesta unánime de la doctrina alemana y la de algunos autores italianos que han tratado este supuesto (PECORELLA) niega que ésta exista en tales casos. PECORELLA, 2006: 335. **Ponen la atención en las medidas:** BRAGHÒ, 2008: 480. CATULLO, 2006: 153. D'ARCANGELO, 2006: 759. D'ARCANGELO, 2008: 1066. FOTI, 2010: 387.

[155] Sigue esta tesis respecto del artículo 197.3 la Sentencia de la Audiencia Provincial de Girona (Sección 4ª) número 358 de 22 de junio de 2015. La doctrina alemana hace referencia al concepto de perceptibilidad (*Wahrnehmbarkeit*) de los datos.

Es irrelevante desde esta perspectiva que el sujeto activo tome conocimiento de los datos o que produzca una interferencia en el funcionamiento del sistema[156]. Igualmente, tampoco queda amparada en el tipo la obtención del control sobre los datos mediante la adquisición de la posesión sobre los mismos[157].

Esta postura privilegia la consideración del delito como un **tipo de peligro**[158], generalmente **abstracto**, y de **mera actividad**[159] en el que el riesgo para el bien jurídico se crea cuando el sujeto ha conseguido penetrar en el sistema, que ahora se encuentra desprotegido. Además, en general este sector lo define como un **delito instantáneo** que se perfecciona en el exacto momento en el que se ha superado la última barrera de protección[160]. Asimismo, también se ha apuntado que se trata de un tipo de **efectos prolongados**, ya que los efectos del delito se alargarían hasta el momento en el que el sujeto abandonara el sistema informático[161].

---

[156] DESTITO et al., 2007: 82. GERCKE y BRUNST, 2009: párrafos 97-99. SCHUHR, 2010: 156. MEIER, 1992: 662. FISCHER, 2015: párrafo 11a. GRÖSELING y HÖFINGER, 2007: 551. WEIDEMANN, 2010: párrafo 16. KRUTISCH, 2004: 125. KINDHÄUSER, 2013: 746 párrafo 5. PARODI y CALICE, 2001: 54. GATTA, 2011: 300. PECORELLA, 2006: 335. SCHUMANN, 2007: 676.

[157] BOSCH, 2014: 1277 párrafo 7.

[158] **Consideran que se trata de un delito de peligro abstracto:** BORRUSO, 1994b: 28. DE SANZO et al., 2009: 896, 898. FONDAROLI, 1996: 311. MERLI, 1993: 126. PECORELLA, 2006: 335. PECORELLA, 2011: 5982. TRENTACAPILLI, 2002: 1283. **En cambio, considera que se trata de un delito de peligro concreto** MAIORANO, 2010: 1357. **Se decantan por la estructura de lesión:** DELPINO, 2003: 584. En España, el artículo 197.3 se consideraba un delito obstáculo: FERNÁNDEZ TERUELO, 2011: 198. MATELLANES RODRÍGUEZ, 2008: 68.

[159] **Delito de mera actividad:** ALIBRANDI, 2011: 1756. DE SANZO et al., 2009: 898. MAIORANO, 2010: 1356. PARODI y CALICE, 2001: 66. PECORELLA, 2011: 5988.

[160] PICA considera que, en realidad, la introducción raramente termina con la acción del acceso, entendiendo que los efectos del delito se extienden en todo el tiempo en el que perdura el mantenimiento del sujeto en el sistema accedido, por todo lo cual concluye que se trata de un **delito permanente** (Pica, 1999: 57-58) **Delito instantáneo:** CARINGELLA et al., 2011: 1054. DESTITO et al., 2007: 89. GAROFOLI, 2013: 648. MAIORANO, 2010: 1357. ?MUCCIARELLI, 1996: 101. PECORELLA, 2011: 5987. RELLA, 2007: 43. VICARIOLI, 2008: 247. Entienden que se trata de un delito de **consumación anticipada** PARODI y CALICE, 2001: 67.

[161] VICARIOLI, 2008: 240. CARINGELLA et al., 2010: 1054. DESTITO et al., 2007: 89.. PECORELLA, 2011: 5987.

c) POSTURA RESTRINGIDA: CONOCIMIENTO DEL CONTENIDO

La corriente más restrictiva, con mayor apoyo que la primera pero en ningún caso mayoritaria, concibe el delito como un tipo de lesión, y subordina la consumación del delito a la **efectiva toma de conocimiento** de los datos, informaciones o programas contenidos en el sistema por el sujeto activo, lo que supondría retrasar la consumación más allá de la eventual superación de las medidas de seguridad, que, por sí misma, no comportaría tal conocimiento.

El punto de inflexión para los partidarios de esta teoría se sitúa en determinar el **grado de conocimiento** que debe haber adquirido el sujeto activo sobre el contenido del sistema. Así, mientras que algunos autores consideran suficiente la mera visualización de datos (en ocasiones sin exigir la superación de las medidas de seguridad)[162], otros consideran que debe haberse adquirido algún género de resolución mental (que no la conciencia plena) sobre una parte relevante de los mismos[163].

---

[162] Esta corriente es seguida unánimemente por la doctrina alemana que, en el primer sentido que ofrece a la § 202a, el de apoderamiento de datos (*verschaffen von Daten*) entienden como una de las posibilidades de comisión la mera toma de conocimiento sobre los datos. En tal sentido se afirma que el delito exige para su consumación la existencia de un verdadero control sobre los datos, y que ello tiene lugar en un apoderamiento inmaterial si el sujeto obtiene conocimiento tanto de forma óptica como acústica sobre datos (KRUTISH) porque tiene disposición de los mismos en tanto información inmaterializada al tenerlos en la cabeza y tener la posibilidad de escribirlos posteriormente (JESSEN). KINDHÄUSER, 2013: §202a RN 5 o pág. 746. ERNST, 2007: 2661. SCHREIBAUER y HESSEL, 2007: 616. SCHUMANN, 2007: 675. FISCHER, 2015: rn 11. KARGL, 2013a: rn 12 o pág. 1413. Drucksache, 1986: 29. HAFT, 1987: 10. KINDHÄUSER, 2013: §202a RN 5 o pág. 746. ,ALTENHAIN y WIETZ, 2013a: 1590. GRÖSELING y HÖFINGER, 2007: 551. LENCKNER y EISELE, 2010: párrafo 10. SCHMITZ, 1995: 483. SCHUHR, 2010: 156. GRAF, 2012: rn. 36. HOYER, 2012: rn. 11. HILGENDORF, 2005: Rn. 16. GRAF, 2012: rn. 50 pág. 196. BOSCH, 2014: rn 6. TAG, 2013: Rn. 8 pág. 1092. GRAF, 2012: 50 o página 196. HILGENDORF, 1996: 704. JESSEN, 1994: 144. MEURER, 1992: 976. SCHMID, 2001: 108. SCHULZE-HEIMING, 1995: 81. LACKNER y KÜHL, 2014: rn. 5. SCHÜNEMANN, 2000: rn 6. RUDOLPHI et al. párrafo 11. LENCKNER y EISELE, 2010: párrafo 10.

[163] CADOPPI et al., 2011: 535-536. CANNATA, 2006: 537. MANTOVANI, 2011: 543, 544, 546. NUNZIATA, 1998: 715. RELLA, 2007: 43. VITARELLI, 2011: 399.

2. TENTATIVA

La configuración del tipo en términos de peligro o de lesión y, con ello, de la interpretación que se realice del verbo acceder, tiene relación no solo con la afirmación de la relevancia de la conducta típica y el momento de la consumación, sino también en la configuración de la tentativa. Así pues, la construcción del delito en términos de peligro conduce al sector doctrinal que defiende esta postura, generalmente, a considerar inadmisible la **tentativa**, pues ello supondría un excesivo adelantamiento de la barrera punitiva[164]. Por el contrario, aquellos autores que consideran el delito como un tipo de lesión la consideran susceptible de punición[165].

Por otra parte, la impunidad de la tentativa resulta criticable en algunos países, donde esta circunstancia contrasta con la previsión de disposiciones específicas que castigan los actos preparatorios[166].

164

a) No admiten la tentativa: ALTENHAIN y WIETZ, 2013b: 1590 párrafo 7. FISCHER, 2013: 1277 párafo 7. ERNST, 2007: 2661. GERCKE y BRUNST, 2009: 69 párrafo 97. HEGER, 2014: 922 párrafo 5. KINDHÄUSER, 2013: § 202a rn 6 o 746. LENCKNER y EISELE, 2010: 1822 párrafo 10. CANNATA, 2006: 538. DOLCINI y MARINUCCI, 2011: 5988. ANTOLISEI, 2008: 247. MUCCIARELLI, 1996: 101. SCHUMANN, 2007: 676. SCHREIBAUER y HESSEL, 2007: 616-617.

b) Sin embargo, admiten la tentativa BOSCH, 2014: 1277 párrafo 7. CARINGELLA et al., 2011: 1054. CECCACCI, 1994: 70. DELPINO, 2003: 585. GAROFOLI, 2013: 648. RELLA, 2007: 834. PARODI y CALICE, 2001: 64, DESTITO et al., 2007: 89. ANTOLISEI, 2008: 240. ALIBRANDI, 2011: 1756. BORRUSO, 1994b: 28. CARINGELLA et al., 2010: 1054. CECCACCI, 1994: 71. DELPINO, 2003: 585. DESTITO et al., 2007: 89. DOLCINI y MARINUCCI, 2011: 5982, 5985, 5987. DE SANZO et al., 2009: 898. MAIORANO, 2010: 1357, 1368. GATTA, 2011: 300. PECORELLA, 2006: 336. PICA, 1999: 57. MELONI, 2012: 2994. GAROFOLI, 2013: 646. MARANI, 2007: 619, 621.

165 **Delito de lesión:** PICA, 1999: 58. NUNZIATA, 1996: 715. PARODI y CALICE, 2001: 64. MANTOVANI, 2011: 546. MARANI, 2007: 622. DESTITO et al., 2007: 82. VITARELLI, 2011: 399. CANNATA, 2006: 537. PECORELLA, 2006: 537. DESTITO et al., 2007: 89. MANTOVANI, 2011: 544-546.

166 Este es el caso de Alemania e Italia. Para una información detallada sobre la regulación de estos países debe remitirse al Capítulo II.

3. VALORACIÓN PERSONAL

La consumación del delito requiere, en mi opinión, haber sobrepasado las dos fases a las que se ha hecho referencia al principio de este apartado, eso es, tanto la fase de contacto con el sistema como la fase de introducción electrónica en el mismo.

Para lograr lo anterior, el sujeto activo deberá superar cuantos medios de protección, físicos o lógicos, le impidan iniciar el diálogo con el sistema, puesto que el tipo penal solo ofrece protección a los sistema informáticos dotados de **medidas de seguridad** (recuérdese que el acceso debe producirse *vulnerando las medidas de seguridad*), tal y como se verá en el Capítulo VI.

La superación de tales medidas otorga al sujeto la **disponibilidad** sobre el sistema, situándole en la condición de acceder u obtener los datos, informaciones y/o programas eventualmente almacenados en el sistema o en alguna parte de éste. Con la adquisición de la disponibilidad se produce la perfección del tipo, sin que sea necesaria mayor incursión o interrupción en su funcionamiento, es decir, sin que sea necesario que el sujeto adquiera el conocimiento sobre los datos, informaciones y programas contenidos en el mismo así como tampoco que ocasione alguna interferencia en su funcionamiento.

Desde esta perspectiva, creo que el delito se configura como un **delito de resultado** y no de mera actividad en el que, tras la desactivación o superación de las medidas de seguridad, el sujeto logra una incursión electrónica en el interior de la memoria interna del sistema obteniendo la disponibilidad sobre el mismo.

Desde este punto de vista, el acceso ilícito constituye también, como un **delito de consumación instantánea** en el que la perfección se produce en el momento y lugar del acceso, y **de efectos prolongados**, pues los efectos se prolongan hasta que el sujeto activo abandona el sistema informático.

En cuanto a la tentativa, en España se regirá por las reglas generales, lo que implica al tratarse de un delito de resultado que ésta será plenamente admisible. En este sentido, todas aquellas acciones que se produzcan en un momento anterior a la adquisición de la disponibilidad sobre el sistema supondrán una imperfecta realización del tipo caerán en el ámbito de la tentativa, acabada o inacabada.

Constituirá tentativa, pues, el simple contacto del sujeto activo con el sistema, así como la superación parcial de las medidas de seguridad, sean éstas lógicas o físicas. En este sentido, respecto de las **medidas de tipo físico dispuestas únicamente en el local,** debe decirse que pueden resultar conflictivos aquellos supuestos en los que tiene lugar la mera introducción de la persona en el lugar donde se encuentra el sistema informático. No obstante, puesto que el objeto material del delito es el sistema informático y no los datos informáticos, el hecho de que el sistema informático esté vacío o que los datos que en él se encuentren estén protegidos no alterarán la consumación del delito, pues el sujeto ya ha adquirido la disponibilidad del sistema.

D) AUTORÍA Y PARTICIPACIÓN: ESPECIAL REFERENCIA A LA ACCIÓN DE FACILITACIÓN DEL ACCESO Y SU RELACIÓN CON EL ARTÍCULO 197 TER

1. AUTORIA Y PARTICIPACIÓN EN EL ACCESO

No existen particularidades especiales en relación con el sujeto activo del delito, pues se trata de un delito común[167]. En la medida en que se trata de un delito de resultado, la conducta típica se puede cometer tanto por acción como por omisión. Sin embargo, deben realizarse al respecto algunas precisiones:

a) MODALIDAD ACTIVA:

El acceso ilícito puede cometerse tanto por un sujeto que es usuario del sistema informático como por un sujeto que no lo es[168], quien puede acceder tanto de forma directa como mediante la intervención de personas interpuestas que faciliten el acceso ayudándole a vencer las medidas de seguridad.

a) Autor que no es usuario del sistema: en este caso cabe destacar la posibilidad de apreciar la autoría mediata en aquellos supuestos en los que se contrata los servicios de un profesional para superar de las medidas de seguridad, y esta desconoce la efectiva intención del sujeto activo[169]. Por el contrario, si éste conociera la voluntad del sujeto, sería autor y el primero inductor[170].

b) Autor que es usuario del sistema: deben distinguirse dos supuestos:

---

[167] En Alemania es definido, no obstante, como un delito especial de carácter negativo (*negatives Sonderdelikt*), pues autor solo será aquel para quien los datos no estén destinados. ALTENHAIN y WIETZ, 2013b: 1592 párrafo 11. BOSCH, 2014: 1279 párrafo 11. FISCHER, 2013: 1363 párrafo 14. GRAF, 2012: 214 párrafo 98.

[168] GALDIERI, 1997: 49.

[169] BOSCH, 2014: 1279 párrafo 11. FISCHER, 2013: 1363 párrafo 14.

[170] BOSCH, 2014: 1279 párrafo 11. FISCHER, 2013: párrafo 14. GRAF, 2012: 215 párrafo 99.

b.1) El usuario del sistema que tenga un poder de disposición sobre la totalidad del sistema será autor del delito debido a la elevación de los casos de participación a autoría que se explicarán en el apartado siguiente[171].

b.2) El usuario del sistema que, teniendo autorización para acceder a determinadas partes del mismo, excede su autorización y accede a partes distintas de las que tiene autorización[172] cometerá, en mi opinión, un acceso ilícito y no una conducta de mantenimiento ilícito si existe vulneración de medidas de seguridad, pues no se trata de una conducta de mera actividad, sino de resultado.

b) MODALIDAD OMISIVA: COMISIÓN POR OMISIÓN

En la medida en que, como he dicho, el delito comentado es un delito de resultado, que se consuma una vez se obtiene la disponibilidad, tiene cabida la comisión por omisión[173]. Esto tendrá lugar ante la concurrencia de medidas de tipo organizativo cuando exista un encargado de custodiar el sistema informático que ostente una posición de garante en relación con el sistema informático, posición que le obliga a responder en caso de que su dolosa desprotección cuando ésta conduzca o facilite la realización del tipo por un tercero[174]. Es posible distinguir dos supuestos:

---

[171] ANARTE BORRALLO y DOVAL PAÍS, 2015: 518. Hasta la reforma de 2015 sería meramente partícipe en aplicación de los artículos 27 a 29 del Código penal, tal y como sucede en otros países. Así en Alemania destacan esta posibilidad: BOSCH, 2014: 1279 párrafo 11. KAISER, 2011: 388. KÜHNE, 2010: 276. SPERNATH, 2010: 308. TRÜG, 2011: 112F.

[172] En sentido similar sobre la regulación alemana, pero debiéndose tener en cuenta que el objeto material son los datos: GRAF, 2012: 214-215 párrafo 98.

[173] ANARTE BORRALLO y DOVAL PAÍS, 2012: 29. Sobre comisión por omisión: ÁLVAREZ GARCÍA, 2008: 45-72. CARBONELL MATEU, 2014: 5-44. CUERDA ARNAU, 2009: 415-436. DOPICO GÓMEZ-ALLER, 2004: 309. ETCHEBERRY ORTHUSTEGUY, 2008: 879-902. GIMBERNAT ORDEIG, 2002. MARTOS NÚÑEZ, 2016: 1 y ss. ROBLES PLANAS, 2012: 18. ROBLES PLANAS, 2013: 1 y ss. ROMEO CASABONA, 1993, SILVA SÁNCHEZ, 1998: 37-42. SILVA SÁNCHEZ, 1989: 367-404, SCHÜNEMANN, 2008: 1609-1630, RUEDA MARTÍN, 2015: 1 y ss.

[174] BOSCH, 2014: 1279 párrafo 11.

a) Si el guarda de seguridad es la única medida de seguridad establecida para impedir el acceso al sistema y éste descuida su cometido posibilitando a un tercero acceder al mismo, la facilitación en la que consiste su intervención es tan próxima al resultado que condiciona la propia producción del hecho.

b) Lo mismo sucede con el sujeto que, debiendo encargarse de la instalación de determinadas medidas de seguridad, incumple su obligación permitiendo el acceso a un tercero. Sin duda, se trata de una aportación anterior a la que sucederá la introducción electrónica en la que consiste el acceso.

En tales casos, el lapso de tiempo entre acción y resultado es prácticamente indiferenciable, de tal forma que la contribución del garante podría considerarse una autoría no ejecutiva o, mínimamente, una cooperación necesaria, que igualmente sería castigada como autoría[175]. Lo anterior se fundamenta en la proximidad de la afectación del bien jurídico y en que el guarda de seguridad es quien mantiene el dominio del hecho, además de en la infracción de su deber de vigilancia dentro de la organización.

[175] Los considera partícipe BOSCH, 2014: 1279 párrafo 11. También, BARTON, 2010, 250.

2. EL CONCEPTO EXTENSIVO DE AUTOR

Los casos de participación deberían presentarse en aquellos supuestos en los que o bien el sujeto ayuda al autor a superar las medidas de seguridad o le proporciona los medios necesarios para acceder al sistema, siempre que éste no sea quien obtiene la disponibilidad sobre éste[176]. En ello se incluiría tanto la participación por acción, como por ejemplo, la facilitación de los códigos de acceso, tanto la comisión por omisión, en aquellos supuestos en los que el sujeto es garante del sistema, generalmente el encargado de una empresa cuyo objeto es garantizar la protección del sistema que incumple dolosamente su función facilitando al autor el acceso al mismo[177].

No obstante, ninguna de estas circunstancias a día de hoy constituye participación, pues, al igual que ocurre en otros delitos, el legislador ha elevado las conductas de participación delictiva a la categoría de autoría. Efectivamente, con la reforma de 2015 se ha previsto un concepto extensivo de autor que engloba tanto los casos de autoría en sentido estricto como los de participación, excluyendo prácticamente la totalidad de las formas de participación. La conducta típica es tan amplia que cualquier contribución causal al fin de facilitación del acceso al sistema se castiga como autoría, coautoría o autoría mediata *ex* artículo 28.1 del Código penal.

---

[176] En sentido similar sobre la regulación alemana, GRAF, 2012: 215 párrafo 99.

[177] En este caso que los criterios de graduación del injusto conducen a una menor intensidad de la intervención del garante, cuando éste sea el encargado únicamente de una medida o una parte no esencial de las medidas de seguridad instaladas. La magnitud del acto del que el garante está encargado dentro de la organización no concreta la realización típica de la conducta de una forma sustancial. El injusto personal de este interviniente no tiene un carácter fundamental en la producción del hecho. Su aportación será coetánea posiblemente a la producción del acceso, pero el grado de probabilidad de la lesión y el grado de lesividad del bien jurídico es muy inferior al comentado en el párrafo anterior. La intensidad de su injusto es no decisiva y por tanto como su intervención en la producción del resultado es mínima, aunque cualitativamente existe una infracción de un deber de vigilancia de la misma intensidad que la anterior, debería, en mi opinión, castigársele como cómplice. BOSCH, 2014: 1279 párrafo 11. ROBLES PLANAS, 2012: 7. En contra, niegan la autoría por comisión por omisión pero aceptan la participación ANARTE BORRALLO y DOVAL PAÍS, 2012: 29.

Así pues, al igual que sucede en otros tipos penales, el acuerdo previo convierte a todos los intervinientes en autores. Podría considerarse, no obstante, como sucede por ejemplo en el delito de tráfico de drogas la figura de la complicidad en aquellos casos en los que la participación es accesoria accidental no necesaria, es decir, cuando los hechos se hubieran producido igualmente sin esa colaboración, especialmente en los casos de colaboración mínima de favorecimiento del favorecedor cuando no existe un acuerdo previo.

3. LA ELEVACIÓN A AUTORIA DE LOS ACTOS PREPARATORIOS DEL ACCESO Y SU FACILITACIÓN: EL ARTÍCULO 197 TER

Se han elevado también a autoría los actos preparatorios del acceso y la participación en los mismos, que se castigan separadamente en el artículo 197 *ter*, lo que obliga a examinar conjuntamente ambos preceptos. El artículo 197 *bis* castiga, como se ha visto, el acceso al sistema informático o su facilitación el artículo 197 *ter* sanciona la producción, adquisición, importación o facilitación de programas informáticos en su letra a) o clave de acceso que permitan acceder a la totalidad o a una parte del sistema informático en su letra b) o la facilitación de estas conductas[178].

En principio podría afirmarse que el artículo 197 *ter* castiga los actos preparatorios y las conductas de preparación de los mismos, mientras que la participación directa en la comisión del delito de acceso se castiga en el artículo 197 *bis* apartado 1[179]. No obstante,

---

[178] ***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 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.*

[179] En un sentido similar sobre la regulación alemana se pronuncia BOSCH, 2014: 1279 párrafo 11.

mientras que el apartado a) del artículo 197 *ter* sí prevé un acto preparatorio del acceso ilícito, el apartado b) recoge, en mi opinión, una conducta de participación en el acceso. Cuando un sujeto facilite a otro la clave de acceso que le permita acceder a un sistema informático ajeno su conducta será subsumible tanto en la modalidad de facilitación del artículo 197 *bis* como en la de facilitación del artículo 197 *ter*, produciéndose un concurso de normas a resolver en virtud del articulo 8 del Código penal por el principio de especialidad.

Esta incongruencia típica, a la que se une la ya apuntada en relación con la tentativa, es consecuencia de la transposición del artículo 6 del Convenio sobre Cibercrimen[180] y del artículo 7 de la

---

[180] **Article 6 – Misuse of devices**

1. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right:

> *a) the production, sale, procurement for use, import, distribution or otherwise making available of:*
>
> *i) a device, including a computer program, designed or adapted primarily for the purpose of committing any of the offences established in accordance with Articles 2 through 5;*
>
> *ii) a computer password, access code, or similar data by which the whole or any part of a computer system is capable of being accessed,*
>
> *with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5; and*
>
> *b) the possession of an item referred to in paragraphs a.i or ii above, with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5. A Party may require by law that a number of such items be possessed before criminal liability attaches.*

2. This article shall not be interpreted as imposing criminal liability where the production, sale, procurement for use, import, distribution or otherwise making available or possession referred to in paragraph 1 of this article is not for the purpose of committing an offence established in accordance with Articles 2 through 5 of this Convention, such as for the authorised testing or protection of a computer system.

3. Each Party may reserve the right not to apply paragraph 1 of this article, provided that the reservation does not concern the sale, distribution or otherwise making available of the items referred to in paragraph 1 a.ii of this article.

Directiva[181], los cuales obligan al legislador a incriminar tales conductas, tal y como ya se ha hecho en otros países, como

[181] **Artículo 7 Instrumentos utilizados para cometer las infracciones**

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 o datos similares que permitan acceder a la totalidad o a una parte de un sistema de información.

Alemania[182] o Italia[183], donde tienen disposiciones específicas al respecto. Debe resaltarse, no obstante, que el legislador español ha ido más allá de la normativa supranacional, previendo conductas que no formaban parte de la propuesta de incriminación incluida en ésta, tales como la facilitación de los propios actos preparatorios o el castigo no sólo de los casos más graves sino de todos lo supuestos posibles.

---

[182] **§ 202c Vorbereiten des Ausspähens und Abfangens von Daten**

(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.

[183] **Art. 615-quater. Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici.**

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 617- quater.

Art. 615-quinquies Diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico

Chiunque, allo scopo di danneggiare illecitamente un sistema informatico o telematico, le informazioni, i dati o i programmi in esso contenuti o ad esso pertinenti ovvero di favorire l'interruzione, totale o parziale, o l'alterazione del suo funzionamento, si procura, produce, riproduce, importa, diffonde, comunica, consegna o, comunque, mette a disposizione di altri apparecchiature, dispositivi o programmi informatici, è punito con la reclusione fino a due anni e con la multa sino a euro 10.329.

SECCIÓN 2ª

LA ACCIÓN DE MANTENIMIENTO

3. INTRODUCCIÓN

La segunda de las dos conductas castigadas en el artículo 197.1 *bis* es el mantenimiento en el sistema informático en contra de la voluntad de quien tenga el legítimo derecho a excluirlo. Esta modalidad típica se introdujo de forma totalmente novedosa en el Proyecto de Reforma del Código penal de 2009[1], pasando totalmente desapercibida durante la tramitación parlamentaria del Proyecto de Ley que condujo a la aprobación de la Ley Orgánica 5/2010, de 22 de junio, y viéndose después inalterada por la reforma operada por la Ley Orgánica 1/2015, de 30 de marzo.

Esta falta de atención resulta extensible también a la propia doctrina española, que ha soslayado las importantes incongruencias que su introducción en el tipo supone y, a diferencia de lo que sucede en otros países, no ha realizado ninguna crítica al respecto. Ésta se ha centrado, pues, en analizar la conducta desde una perspectiva sistemática y comparada, intentando únicamente en localizar cuál es su origen jurídico, sin hacerse todavía eco de los innumerables problemas interpretativos que plantea.

Teniendo en cuenta la problemática apuntada, a ambos aspectos se prestará atención en la presente Sección de este Capítulo, que se dedicará, primero, al análisis de su origen y contenido típico, pero después a la presentación de una crítica detallada a los efectos de proponer su derogación. Adentrémonos, pues, a continuación cual es mi visión personal sobre esta modalidad típica.

---

[1] Efectivamente, esta segunda modalidad aparece sorpresivamente en el Proyecto de 2009, pasando desapercibida durante toda la tramitación parlamentaria -en la que sólo se presta atención a la modificación producida en el apartado 8 relativa a la comisión del delito en el seno del fenómeno conocido como delincuencia organizada y la responsabilidad penal de las personas jurídicas- que conducirá a la aprobación (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)

II. ORIGEN

La doctrina española[2] quiso ver en su inclusión la influencia del **artículo 615 *ter* del Código penal italiano**[3], el cual fue introducido ya en el año 1993[4]. Sin negar que el legislador español haya copiado directamente la literalidad del precepto mencionado, no puedo dejar de poner de relieve que no creo que el legislador italiano sea el **"creador"** originario de la conducta, puesto que Francia[5] ya disponía de un precepto muy similar en su Código penal un año antes de la tipificación del mantenimiento ilícito en el sistema por parte de Italia[6]. A mi parecer, su verdadero origen, quiera llamársele indirecto, se sitúa en la **§ 1030 (a) del Código Federal de Estados Unidos**[7], que, si bien no castiga el mantenimiento en el sistema en contra de quien ostente un legítimo derecho de exclusión, sanciona el exceso de aquel que tiene autorización para acceder tan solo a una parte del sistema.

---

[2] CARRASCO ANDRINO, 2010: 250. MORALES PRATS, 2011: 821.

[3] *Art. 615-ter. Accesso abusivo ad un sistema informatico o telematico.*
*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.*

[4] Concretamente, fue la Legge 23 dicembre 1993, n. 547 *di modificazioni ed integrazioni alle norme del codice penale e del codice di procedura penale in tema di criminalità informatica* la que criminalizó, entre otros comportamientos relativos a la delincuencia informática, el acceso ilícito en Italia.

[5] Article 323-1 *Le fait d'accéder ou de se **maintenir**, frauduleusement, **dans tout ou partie d'un système de traitement automatisé de données** est puni de deux ans d'emprisonnement et de 60 000 € d'amende*.

[6] En Francia, fue la Loi n° 92-685 du 22 juillet 1992 *portant réforme des dispositions du code pénal relatives à la répression des crimes et délits contre les biens* la que codificó el acceso ilícito a un sistema informático en el Código penal.

[7] 18 U.S. Code § 1030 - Fraud and related activity in connection with computers
(a) (…) *accesses a protected computer without authorization, or **exceeds authorized access*** (…) Esta Sección fue introducida en Título 18 del Código Penal Federal de Estados Unidos de América en 1986 a través de la *Counterfeit Access Device and Computer Fraud and Abuse Act*, conocida como *Computer Fraud and Abuse Act (CFAA)*, si bien la incriminación del fenómeno de la delincuencia informática empezó en este país con la *Comprehensive Crime Control Act* de 1984.

A) "EXCESO DE AUTORIZACIÓN" EN LA SECCIÓN 1030 DEL CÓDIGO PENAL FEDERAL DE ESTADOS UNIDOS

En el supuesto conocido en Estados Unidos de América como exceso en la autorización, el sujeto activo ostenta un título jurídico que le permite acceder a la totalidad del sistema pero con unas facultades concretas. En lugar de criminalizar este supuesto con base en la formulación de una nueva modalidad típica, la Sección 1030 del Código Penal Federal de los Estados Unidos de América hace descansar estructuralmente la tipicidad de la acción en el consentimiento[8]. Así, la acción siempre es la misma: el acceso, pero la responsabilidad penal se activa tanto cuando el sujeto accede al sistema en ausencia de consentimiento, esto es, sin autorización (*without authorization*), como cuando, gozando del mismo, existe un exceso en la autorización concedida (*exceeding authorized access*)[9].

La literatura norteamericana vincula directamente la acción con el término de *insiders* (por contraposición al acceso sin autorización que sería cometido por *outsiders*), es decir, aquellos sujetos que ostentan algún género de facultad de acceso sobre el sistema informático y la información[10]. Aunque esta conducta tiene

---

[8] KARAGIANNOPOULOS, 2014: 466.

[9] Como se ha indicado anteriormente, esta segunda modalidad de comisión de la acción de acceso ilícito fue introducida en la legislación federal de los Estados Unidos de América a través de la *Computer Fraud and Abuse Act de 1986*, pues la *Comprehensive Crimen Control Act* de 1984 que la precedía como primera respuesta del país en contra del fenómeno denominado en el país como *hacking* informático nada contenía al respecto. La expresión *exceeding authorized access* reemplaza la originaria redacción que era descrita en la Ley de 1984, la cual era descrita como: *having accessed a computer with authorization, uses the opportunity such access provides for pursposes to which authorization does not extend*.

[10] KARAGIANNOPOULOS, 2014: 466. DOYLE y BARLETT WEIR, 2006: 4. MARSHALL y BAILI, 2011:.

su sede original en el seno de una relación laboral[11], también se plantea esta conducta en el contexto de las relaciones contractuales de carácter civil[12].

Uno de los puntos más importantes es la distinción entre la eliminación del consentimiento y el exceso de autorización. Así pues, se considera que la autorización cesará cuando un empleado adquiere sin conocimiento del empleador intereses adversos o en otro sentido quiebra la lealtad que debe a éste, de modo que el motivo por el que un empleado usa el ordenador de su trabajo determina la existencia de autorización[13]. No obstante, la jurisprudencia es contradictoria porque en Brekka vs. LVRC Holdings el órgano judicial considera que el exceso de autorización depende de las concretas acciones que el empleado realiza para poner limitaciones explícitas al uso de la autorización dada a sus empleados, siendo que la *Computer Fraud and Abuse Act* no sugiere nada a los efectos de determinar la responsabilidad del empleado en atención a la violación de un deber legal de lealtad al empleado[14].

En cualquier caso, incluso en Estados Unidos de América esta conducta es muy discutida, siendo su interpretación extremadamente controvertida, llegando a abogarse por su derogación[15].

---

[11] Habitualmente los límites de la autorización para los *insiders* vendrán limitados por las instrucciones y el uso de potestades por el empleador. En tales casos, cuando el uso por parte del empleado de su autorización es inconsistente en relación con las instrucciones proporcionadas por el empleador, el empleado está excediendo su autorización. Véase Caso United States vs. Morris, Caso United States vs. Czubinshki, Caso Brekka y Nosal KARAGIANNOPOULOS, 2014: 472.

[12] Ello sucederá cuando se de un exceso en relación con los términos de uso de páginas web y servicios online. Véase Caso EF Cultural Travel BV vs. Explorica Inc. KARAGIANNOPOULOS, 2014: 472.

[13] La autorización se ve eliminada en el momento en que el empleado actúa en contra de los intereses del empleador. Caso Shurgard Centers, Inc. vs. Safeguard Self Storage, Inc. KARAGIANNOPOULOS, 2014: 475. MARSHALL y BAILI, 2011: 4.

[14] Caso Brekka vs. LVRC Holdings KARAGIANNOPOULOS, 2014: 481.

[15] Explica KARAGIANNOPOULOS que el concepto de autorización está creando más problemas y controversias que soluciones por lo que respecta a la delincuencia informática. KARAGIANNOPOULOS, 2014: 508. MARSHALL y BAILI, 2011: 10.

B) MANTENIMIENTO ILÍCITO EN EL ARTÍCULO 615 *TER* DEL CÓDIGO PENAL ITALIANO

En el ámbito penal italiano, la conducta de mantenimiento ilícito en un sistema informático resulta equiparable a la modalidad pasiva del allanamiento de morada, puesto que el legislador italiano creó esta figura a imagen y semejanza de los delitos contra la inviolabilidad del domicilio[16].

Consiste en la permanencia en el sistema informática en contra de la voluntad del titular del *ius excludendi*. Se trata de una conducta alternativa y subsidiaria a la de introducción en el sistema informático, que se produce cuando el acceso previo ha sido lícito y sin vulneración de medidas de seguridad[17].

Dentro de esta modalidad típica se insertan cuatro supuestos: en primer lugar, un abuso de legitimación que se ostenta sobre el sistema informático al ir más allá de los límites modales o temporales[18]; revocación del consentimiento[19]; acceso involuntario o

---

[16] Relazione Ministeriale di accompagnamento alla legge n. 547/1993, pág. 9.

[17] Explica CANNATA que la relevancia penal de la conducta de permanencia no es, en efecto, necesariamente autónoma en relación con la de acceso. Sólo en la hipótesis en la cual el sujeto activo se ha introducido lícitamente en el interior del sistema protegido para poder mantenerse ilícitamente en el mismo entrará en aplicación el artículo 615 *ter* del Código penal italiano. Si, por el contrario, el sujeto activo se introduce ilícitamente en un sistema informático dotado de medidas de seguridad y se mantiene en él por un cierto periodo de tiempo, éste responderá por el delito del artículo 615 *ter* no en atención a la modalidad de permanencia sino a la de acceso ilícito, puesto que para la perfección del delito se tendrá en cuenta la propia consumación del acceso, quedando el anterior absorbido en este. CANNATA, 2006: 539.

[18] BORRUSO, 1994: 32. CUOMO y RAZZANTE, 2009: 97. DE SANZO et al., 2009: 898. MONACO, 2011: 2334. PICA, 1999: 41. MAIORANO, 2010: 1357. CUOMO, 2000: 300. PECORELLA, 2006: 349. CANNATA, 2006: 450. GATTA, 2011: 301. MUCCIARELLI, 1996: 101. PICA, 1999: 41. RELLA, 2007: 43.

[19]MAIORANO, 2010: 1356. MARANI, 2007: 618. MUCCIARELLI, 1996: 100. VICARIOLI, 2008: 246. PICA, 1999: 41-42.

casual de buena fe con mantenimiento doloso[20]; y el abuso de autorización excepcional para la realización de unas operaciones muy concretas[21].

La doctrina italiana equipara la conducta a la modalidad pasiva del delito de allanamiento de morada, configurando como un delito de mera actividad que se consuma con la simple permanencia en el sistema sin consentimiento del titular o de los titulares del mismo[22] y como un tipo de carácter permanente, puesto que sus efectos se prolongan hasta el abandono del sistema por el sujeto activo[23].

---

[20] El sujeto debería, una vez advertida su presencia lícita en el sistema cerrar la conexión o buscar el camino de salida. BORRUSO, 1994: 32. CANNATA, 2006: 450. PECORELLA, 2011: 5987. PECORELLA, 2011: 351. FONDAROLI, 1996: 312. MARANI, 2007: 618. VICARIOLI, 2008: 246.

[21] PARODI, 1998: 1040. PECORELLA, 2006: 351.

[22] La perfección típica se produce de igual forma que en el delito de allanamiento de morada con la mera acción de permanecer en la morada sin que sea necesario ningún efecto o resultado adicional. CANNATA, 2006: 451. PARODI, 1998: 1040.

[23] CARINGELLA et al., 2011: 1054. DESTITO et al., 2007: 89. GAROFOLI, 2013: 648. RELLA, 2007: 43.

III. CONTENIDO TÍPICO

Esta conducta guarda seria semejanza con el allanamiento de morada pasivo[24]. En realidad, como se ha expuesto, lo que se está castigando es el mero uso ilegítimo del sistema informático[25].

A) SUPUESTOS

Pueden darse cuatro supuestos:

a) Abuso modal o temporal del acceso concedido: En primer lugar, el contenido de la acción podría suponer la utilización del sistema para un fin distinto al autorizado, o bien por continuar realizando búsquedas u operando en el sistema o servirse de cualquier modo de éste tras haber accedido a éste de forma legítima, o bien por quebrantar las condiciones de acceso a las cuales el titular del derecho de exclusión ha subordinado el acceso[26], abusando de legitimación que se ostenta sobre el sistema informático al ir más allá de los límites modales o temporales concedidos por aquél[27].

b) Revocación del consentimiento: una segunda modalidad de la conducta estaría integrada por el comportamiento omisivo de aquel que, habiendo accedido con autorización del titular del sistema, se mantiene en la utilización del sistema

---

[24] El allanamiento de morada pasivo está recogido en el artículo 202 del Código penal, que lo define como mantenerse en una morada ajena en contra de la voluntad de su morador. Se trata de un comportamiento de naturaleza omisiva en el que el sujeto activo contraviene la voluntad del sujeto pasivo de abandonar la morada HERNÁNDEZ PLASENCIA, 2004: 876 párrafos 202-204.

[25] MAIORANO, 2010: 1357. CUOMO, 2000: 300. PECORELLA, 2006: 349.

[26] Al igual que en el allanamiento de morada pasivo, el acceso previo tiene que haber sido lícito, motivo por el cual se afirma que la conducta de acceso es ley principal respecto a la de mantenimiento. CANNATA, 2006: 450. GATTA, 2011: 301. MUCCIARELLI, 1996: 101. PICA, 1999: 41. RELLA, 2007: 43.

[27] La norma castiga o bien la superación de los límites de temporalidad expresos determinados por la voluntad del titular o bien a quien ostentando un título para acceder al sistema, utiliza a éste para una finalidad diversa a aquella que ha sido consentida. BORRUSO, 1994: 32. CUOMO y RAZZANTE, 2009: 97. DE SANZO et al., 2009: 898. MONACO, 2011: 2334. PICA, 1999: 41.

informático una vez que este ha revocado el consentimiento inicialmente prestado[28].

c) Acceso involuntario o casual con mantenimiento doloso: también podría darse el caso de que el sujeto activo se introdujera de forma casual o involuntaria en el sistema pero, estando su conducta hasta este punto amparada en el error de tipo, éste decidiera dolosamente de forma sobrevenida permanecer en el sistema tras advertir que no disponía de consentimiento que le autorizara al acceso y, por consiguiente, tampoco a permanecer en él[29].

d) Autorización excepcional: algunos autores hacen referencia a un último supuesto que, a mi juicio, es perfectamente subsumible en el primero, del que únicamente se diferencia en el carácter habitual de la permisión que a aquel compete, y es el caso en el que se ha autorizado el acceso únicamente para ciertos aspectos excepcionales y para la realización de unas operaciones muy concretas y por un tiempo estrictamente determinado[30].

---

[28] Para PICA, en cambio, este comportamiento siempre es activo, nunca omisivo, porque la voluntad de la norma está integrada por la petición de abandono por parte del titular del sistema y la acción de mantenimiento voluntario del sujeto activo del delito. MAIORANO, 2010: 1356. MARANI, 2007: 618. MUCCIARELLI, 1996: 100. VICARIOLI, 2008: 246. PICA, 1999: 41-42.

[29] El sujeto debería, una vez advertida su presencia lícita en el sistema cerrar la conexión o buscar el camino de salida. BORRUSO, 1994: 32. CANNATA, 2006: 450. PECORELLA, 2011: 5987. PECORELLA, 2011: 351. FONDAROLI, 1996: 312. MARANI, 2007: 618. VICARIOLI, 2008: 246.

[30] PARODI, 1998: 1040. PECORELLA, 2006: 351.

B) DEFINICIÓN DE LA CONDUCTA

Todos los anteriores supuestos pueden resumirse en una frase, que es la que caracterizará de forma común a la conducta típica y marcará el momento consumativo del delito, el mantenimiento punible tendrá lugar, cuando la introducción en el sistema informático se haya producido de forma lícita, motivo por el cual no existe acceso ilícito, y en cambio, el sujeto permanezca en el sistema en contra de quien tenga un legítimo derecho de exclusión sobre el mismo[31].

C) CONSUMACIÓN

Al igual que el delito de allanamiento de morada, el mantenimiento ilícito en el sistema informático se configura como un delito de mera actividad que se consuma con la simple permanencia[32] en el sistema sin consentimiento del titular o de los titulares del mismo[33], en el que se exige también una intrusión electrónica[34]. También resulta extrapolable la configuración del delito como un tipo de carácter permanente, puesto que sus efectos se prolongan hasta el abandono del sistema por parte el sujeto activo[35].

---

[31] CANNATA, 2006: 450.

[32] La perfección típica se produce de igual forma que en el delito de allanamiento de morada con la mera acción de permanecer en la morada sin que sea necesario ningún efecto o resultado adicional. CANNATA, 2006: 451. PARODI, 1998: 1040.

[33] Véase Capítulo VII.

[34] En sentido similar, MORALES PRATS, 2011: 509.

[35] En contra, DESTITO, DEZZANI y SANTORIELLO consideran que se trata de un delito instantáneo de efectos prolongados para ambas modalidades, que se perfecciona en el momento y lugar del acceso o la permanencia y cuyos efectos se prolongan hasta que el sujeto abandona el sistema informático. CARINGELLA et al., 2011: 1054. DESTITO et al., 2007: 89. GAROFOLI, 2013: 648. RELLA, 2007: 43.

A los efectos de terminar de aclarar los aspectos relativos a la consumación del delito, debe hacerse expresa mención a dos cuestiones:

a) Voluntad manifiesta del titular: como se verá en el correspondiente capítulo[36], no es necesario para la consumación de la conducta de mantenimiento que el titular del derecho de exclusión manifieste su voluntad expresa de ejercitarlo, pues es suficiente con que pueda eliminarse toda duda de que existió una voluntad tácita del titular dirigida a la exclusión del sujeto activo de la permanencia en el sistema[37]. Ello se traduce, por tanto, en una constancia expresa, que no manifestación expresa, de la ausencia de consentimiento por parte del titular de algún derecho sobre el sistema[38].

b) Conocimiento del contenido del sistema: para la consumación del delito tampoco sería necesaria una incursión especifica en el contenido del sistema o la interferencia de su funcionamiento[39].

---

[36] Véase Capítulo VII.

[37] Cierto sector de la doctrina exige, no obstante, como presupuesto, además de la legítima incisión del sujeto en el sistema, una sucesiva voluntad manifiesta de expulsión del titular. No obstante, como pone de relieve MARANI, el delito podrá consumarse también en el caso de que la voluntad del titular no sea manifestada expresamente, más sea intuidle de la introducción o de la permanencia realizada de forma clandestina o con engaño. En tales supuestos, afirma, el delito se consuma en el momento en que se hace patente la exclusión manifiesta del titular del derecho, que puede haber incluso sido tácita y revocarse después. En contra, CUOMO, 2000: 2990. CUOMO y RAZZANTE, 2009: 97. DELPINO, 2003: 585. LUSITANO, 1998: 1923. A favor, MARANI, 2007: 618, 621. PECORELLA, 2006: 351-352. En España sobre allanamiento de morada: MORALES PRATS, 2010: 513. JORGE BARREIRO, 1987: 67. SANZ MORÁN, 2006: 334. En contra MUÑOZ CONDE.

[38] CANNATA, 2006: 538. VICARIOLI, 2008: 247.

[39] Por supuesto, resulta coherente para aquellos autores que han defendido que se trata de un delito de lesión que entiendan en este caso también la exigencia de conocimiento posterior de la información del sistema informático para la consumación de esta segunda modalidad típica. MANTOVANI, 2011: 544, 546.

IV. CRÍTICAS

La conducta de mantenimiento resulta criticable desde una doble perspectiva: por una parte, la propia tipificación de esta conducta resulta muy discutible desde el prisma del principio de ofensividad; por otra, con independencia de lo anterior y teniendo en cuenta la redacción vigente, dos son las objeciones que puede hacerse a este comportamiento, el primero de ellos su ubicación sistemática, el segundo la indebida restricción de la conducta. Véase con más detenimiento cada una de estas críticas:

A) CRÍTICA A LA TIPIFICACIÓN DE LA CONDUCTA: AUSENCIA DE LESIVIDAD DE LA ACCIÓN

El mantenimiento punible tendrá lugar cuando la introducción en el sistema informático se haya producido de forma lícita y, a continuación por cualquiera de las razones expuestas el sujeto permanezca en el sistema en contra de quien tenga un legítimo derecho de exclusión sobre el mismo[40]. Teniendo en cuenta lo anterior, se pude decir que, en realidad lo que se está castigando es el mero uso ilegítimo del sistema informático[41], algo que me parece totalmente censurable conforme a los principios de ofensividad y de intervención mínima, pues esta acción en nada perjudica el disfrute de la informática por el ciudadano ni, en caso de afirmar que sea así, no se trata de un ataque grave al mismo[42]. Entretanto, para reducir los efectos negativos de su punición a aquello que sea estrictamente necesario en términos de utilidad social general, me parece adecuado que los órganos jurisdiccionales usen el principio de insignificancia cuando consideren que una conducta no afecta al bien jurídico protegido por el tipo penal, por la escasa gravedad de la misma[43].

---

[40] CANNATA, 2006: 450.

[41] MAIORANO, 2010: 1357. CUOMO, 2000: 300. PECORELLA, 2006: 349.

[42] En Italia, PECORELLA señala que relevancia penal de la conducta debe depender de la idoneidad de ésta para crear un peligro para el bien jurídico. Sin embargo, ello supondría, a mi juicio, atribuir al delito una naturaleza de peligro concreto y no de peligro abstracto PECORELLA, 2011: 5982.

[43] SILVA SÁNCHEZ, 1992, 242.

B) CRÍTICAS A LA REDACCIÓN VIGENTE

1. UBICACIÓN SISTEMÁTICA

El comportamiento típico adquiere sentido de acuerdo con la configuración que de ella han realizado el legislador italiano y el americano, cada una en sus respectivos términos, pero ningún sentido puede ofrecérsele en el Código penal español.

El mantenimiento ilícito en un sistema informático tal y como ha sido concebido en el Código penal español tiene visos de lo que podría denominarse allanamiento de morada informática de carácter pasivo. Me refiero a que en ella se mantiene la esencia que el legislador italiano le confirió al incriminar el acceso ilícito en el seno de los delitos de contra la inviolabilidad del domicilio, al considerarla una conducta atentatoria contra el domicilio informático[44]. Así pues, cabría distinguir una modalidad de carácter activo, el acceso, y una modalidad de carácter pasivo, el mantenimiento en el sistema.

La coherencia en el ordenamiento italiano de ambas conductas es adecuada por su ubicación sistemática entre los delitos contra la inviolabilidad del domicilio, pero en el ordenamiento español resulta distorsionada por cuanto si éste hubiera sido el deseo del legislador, hubiera incluido el delito en el Capitulo II del Título X y no en el Capítulo I, pues la inviolabilidad del domicilio se ha configurado como un derecho autónomo de la intimidad tanto a nivel constitucional como en el ámbito penal, ello sin valorar la propia introducción del tipo entre los delitos contra la intimidad[45].

---

[44] A través de una no llena de dudas reformulación del tradicional derecho a la inviolabilidad del domicilio. Cabe resaltar también que el la Recomendación 89 (9) proponía como bien jurídico protegido en el delito el domicilio informático, por tanto me parece ésta la causa más probable, por lo que entre el origen de Estados Unidos y la legislación continental debe introducirse esta variable. Recuérdese lo que se dijo en los Capítulo I y II.

[45] Uno de los problemas que se han solventado con la reforma llevada a cabo por la Ley Orgánica 1/2015, de 3 de marzo, es el hecho de que el objeto material del delito no coincidía en una y otra modalidad.

Por lo que respecta a la Sección 1030 del Código Federal de Estados Unidos, podría apuntarse que en este país el exceso de autorización se vincula al consentimiento y a la tendencia interna de obtención de información. Ello significa que, si bien se hace recaer en la tipicidad la relevancia típica de un hecho, la acción siempre será la misma: el acceso ilícito, lo que veta la subsunción en el tipo penal de comportamientos con un injusto distinto tal y como ocurre en la permanencia ilícita.

2. INDEBIDA RESTRICCIÓN DE LA CONDUCTA

La *ratio* de la incriminación en la permanencia ilícita se cimienta en la idea de que resulta necesario ofrecer protección al titular del sistema también en aquellos supuestos en los que el peligro se deriva del hecho de que el sujeto activo ya se encuentra en el interior del mismo como consecuencia de un acceso previo lícito[46]. En este sentido, la previsión típica de esta conducta debería permitir arbitrar una protección global al sistema frente a los peligros que pudieran dimanar no ya de quien accede ilícitamente a él *ab initio*, sino del comportamiento de quien, inicialmente autorizado, ponga en peligro el bien jurídico protegido por el delito[47].

En el ámbito del artículo 197.1 *bis* se han previsto una serie de elementos comunes a las dos conductas típicas, entre los que en este momento cobra relevancia la vulneración de medidas de seguridad. Si se considera que el mantenimiento debe haberse llevado a cabo vulnerando medidas de seguridad, esta modalidad deviene inaplicable, ya sea por entenderse absorbida en el propio acceso cometido vulnerando medidas de seguridad, como un acto posterior impune o, si se quiere, en tanto parte de la fase de agotamiento del delito. En consecuencia, la única interpretación que permite adquirir cierto sentido a la acción supone desvincularlo de ésta, entendiendo

[46] CANNATA, 2006: 220. PECORELLA, 2006: 350.

[47] CANNATA, 2006: 451.

que se castiga únicamente la permanencia ilícita tras un previo acceso lícito[48].

[48] Con base a este principio se crea una mayor adecuación de la conducta al principio de ofensividad, pues se limita el castigo del tipo a aquellas permanencias no autorizadas que efectivamente supongan la creación de un peligro idóneo para el bien jurídico. Esta precisión resulta de todo punto indispensable para evitar que a esta hipótesis vengan reconocidos todos los supuestos de utilización indebida del sistema informático por parte del sujeto activo, que no constituyen un acceso ilícito en sentido estricto porque no compran un acceso ilícito a una área protegida del sismte BERENGHELLA y BLAIOTTA, 1995: 2335. PECORELLA, 2006: 350. PECORELLA, 2011: 5982.

CAPITULO V

EL OBJETO MATERIAL DEL DELITO EN EL ACCESO ILÍCITO

I. INTRODUCCIÓN

El presente Capítulo se dedica al estudio del objeto material de la acción en el delito de acceso ilícito a un sistema informático. Se divide en dos partes, cada una de las cuales se corresponde con la vigencia de la descripción típica vigente durante las dos reformas que han afectado al precepto: la primera, operada por la Ley Orgánica 5/2010, de 22 de junio, que introdujo el tipo penal de acceso ilícito y, la segunda, por la Ley Orgánica 1/2015, de 30 de marzo, que modificó su redacción.

La configuración del objeto material del delito tras la reforma operada por la Ley Orgánica 5/2010, de 22 de junio, era una de las principales incongruencias típicas a resaltar en la infracción penal, ello por dos razones fundamentales:

a) Por un parte, el legislador transpuso el delito de acceso ilícito como un tipo de equivalencia con el delito de descubrimiento y revelación de secretos. Tan forzada ubicación sistemática obligó a modificar el objeto material para adaptarlo al Título que le serviría de acogida: el relativo a los delitos contra la intimidad. De este modo, mientras la normativa supranacional hacía referencia a un acceso a todo o parte de un sistema informático, el Código penal español aludía a acceso a datos y programas informáticos contenidos en todo o en parte de un sistema informático. Lo anterior suponía que era el contenido del sistema –los datos– y no el continente –el propio sistema– el que ostentaba la protección penal.

b) Por otra parte, la segunda características a destacar, también derivada del desacertado encaje propiciado por el legislador al acceso ilícito era la ausencia de uniformidad en el objeto material de las acciones previstas en él. Pues bien, teniendo en cuenta que el legislador español lo configuró como un tipo mixto alternativo, cada una de las dos conductas poseía un objeto material distinto, pues el mantenimiento se vinculaba al propio sistema informático.

La previsión de un objeto material distinto, unida a la ubicación sistemática del precepto, además se suponer un incumplimiento de la normativa supranacional, planteaba multitud de conflictos interpretativos, entre ellos el relativo a la propia delimitación del alcance y contenido del objeto material del delito. Así pues, acertadamente y, además, en el sentido que yo misma había propuesto en trabajos anteriores[1], el legislador ha modificado con la reforma operada por la Ley Orgánica 1/2015, de 30 de marzo, tanto la ubicación sistemática del precepto como el objeto material de la conducta de acceso, que ahora es el sistema informático en ambas modalidades típicas.

Esta modificación del objeto material ha dotado de una mejor coherencia al tipo, que ahora, efectivamente, es un tipo mixto alternativo en el que ambas acciones comparten un objeto material común, y, además, ha supuesto la mejor adaptación del mismo a las exigencias derivadas de la normativa supranacional, puesto que se han solventado los problemas derivados del hecho de que el acceso a un sistema informático puede implicar no solo el acceso a datos sino también a otros componentes del mismo, a los que se estaba vetando cualquier tipo de protección con una previsión típica únicamente vinculada al concepto de dato.

Pero para poder reseñar los avances mencionados, es necesario primero tratar el objeto material del delito conforme a la redacción otorgada por la Ley Orgánica 5/2010, de 22 de junio, para después poder estudiar el concepto de sistema informático como objeto material de acuerdo a la nueva descripción legal de la Ley 1/2015, de 30 de marzo y así conocer el estado actual de la cuestión y en qué aspectos ha mejorado la reforma el objeto material. Es por ello que el presente Capítulo se divide, nuevamente en dos Secciones, la primera dedicada a estudiar el objeto material conforme a la reforma de 2010, la segunda, que presenta la reforma de 2015.

---

[1] MONTSERRAT SÁNCHEZ-ESCRIBANO, 2014: 233-254. MONTSERRAT SÁNCHEZ-ESCRIBANO, 2015: 295-322.

SECCIÓN 1ª

EL OBJETO MATERIAL DEL DELITO DE ACCESO ILÍCITO EN LA REFORMA OPERADA POR LA LEY ORGÁNICA 5/2010, DE 22 DE JUNIO

I. INTRODUCCIÓN

Conforme a la redacción del tipo otorgada por Ley Orgánica 5/2010, de 22 de junio, el objeto material del delito en la modalidad de acceso eran los datos y programas informáticos contenidos en un sistema informático. España no fue el único país que optó por proteger los datos en lugar del sistema informático en la línea iniciada por Alemania, país pionero en la aprobación de legislación en la materia, y seguida por no pocos de los países signatarios del Convenio, algunos de los cuales incluso han adoptado definiciones más o menos cercanas a las recogidas en el Convenio y la Directiva[2].

Como ya se expuso anteriormente[3], la característica definitoria de los datos informáticos según la normativa internacional y comunitaria es su susceptibilidad de tratamiento informático, sin que ninguna otra nota conduzca a la restricción o limitación de tal concepto. Así pues, cabría englobar dentro de dicha noción cualquier representación informática respecto de la que es viable un procesamiento automatizado, ello con independencia de formato, tipología o contenido.

---

[2] Recuérdese, pues, brevemente el concepto de dato informático de una y otra norma:

1. El Convenio sobre Cibercrimen define dato informático como *toda representación de hechos, informaciones o conceptos expresados bajo una forma que se preste a tratamiento informático, incluido un programa destinado a hacer que un sistema informático ejecute una función.*
2. La Directiva 2013/40/UE define datos informáticos 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.*

Los Estados que adoptan los datos como objeto son Alemania, Australia, Bulgaria, Dinamarca, Georgia, Grecia, Islandia, Malta, Moldavia, Noruega y Rusia, si bien Bélgica, Bosnia Herzegovina, Croacia y Finlandia ofrecen tutela tanto al sistema como a los datos.

Un desarrollo más amplio sobre esta cuestión así como el estudio detallado sobre la regulación de cada uno de estos países puede verse en el Apartado X del Capítulo II.

[3] Véase Capítulo I.

Concretamente por lo que se refiere a España, la Ley Orgánica 5/2010, de 22 de junio, introdujo el acceso ilícito en el apartado 3 del artículo 197 del Código penal como un tipo de equivalencia en relación con el delito de descubrimiento y revelación de secretos. Así, al igual que en los demás apartados del precepto, el objeto material del delito eran los datos, a los que en este caso se les atribuía como característica que se hallaran contenidos en todo o en parte de un sistema informático. En mi opinión, aunque con tal expresión el legislador pretendía concretar el concepto de dato en la redacción típica y, con ello, deslindarlo de los datos que hallaban protección por medio de los demás párrafos, en realidad se trataba de dos notas que no aportaban demasiado:

> **a) Datos contenidos en un sistema informático:** cabía preguntarse si sería posible encontrar un dato que fuera informático y que no se hallara contenido en un sistema informático, puesto que pueden existir datos que no tengan la característica de informáticos y que sí se encuentren fuera del sistema informático, pero precisamente lo que caracteriza a los datos informáticos es que estén contenidos en el sistema informático. En consecuencia, a mi modo de ver, el inciso contenidos en un sistema informático resultaba totalmente prescindible porque no aportaba nada a la delimitación de cuáles eran los datos que debían entenderse englobados en el apartado 3 del artículo 197, siendo una reiteración superflua de la idea de dato informático.
>
> **b) Datos contenidos en todo en parte del sistema:** Que dichos datos se hallaran contenidos en todo o parte del sistema informático tampoco podía considerarse como un aspecto relevante de la definición de dato, por una parte, porque todos los datos se hallan contenidos en una parte del sistema sin que ello sea algo sustancial para definirlos, por otra, porque afirmar que un solo dato puede contenerse en todo el sistema informático me parece absolutamente exagerado y materialmente imposible.

Rechazada cualquier relevancia de las dos notas que se utilizaban para delimitar la noción de dato, la única forma de poder establecer cuáles eran los datos informáticos a los que se refería el apartado 3 del artículo 197 consistía en la realización de una interpretación sistemática a efectos de establecer su contenido de forma global en el precepto, ya que, como muy bien señala MORALES PRATS, éste contiene múltiples tipos básicos y agravados, expresados a través de una atormentada e inacabable redacción[4]. Por este motivo, considero muy ilustrativo la realización de una tabla introductoria con el nuevo encuadre a partir de 2010 del artículo 197 en su conjunto:

> **a) Artículo 197.1:** datos contenidos en documentos electrónicos, efectos personales y datos de las telecomunicaciones.
>
> **b) Artículo 197.2:** datos informáticos que la doctrina ha denominado automatizados por estar contenidos en un registro o un archivo de datos reservados de carácter personal o familiar ya sea público o privado.
>
> **c) Artículo 197.3:** datos y programas informáticos contenidos en un sistema informático.
>
> **d) Artículo 197.5 (hoy .6):** datos especialmente sensibles a los que la doctrina se ha referido como integrantes del núcleo duro de la intimidad: ideología, religión, creencias, salud, origen racial o vida sexual.

Tomando en consideración que el hecho de ser un dato informático es una característica predicable de los datos a los que se refieren los apartados 1, 2 y 5, la previsión típica del apartado 3 era

[4] MORALES PRATS, 2008: 453.

coincidente con la de los apartados anteriores[5], suponiendo no solo la ampliación de la esfera de protección de los datos a los que éstos se referían[6], sino, a mi juicio, el completo cierre del ámbito de tutela de la intimidad. De ello se desprendía la existencia de un concurso de normas entre los distintos párrafos del artículo 197 y el introducido apartado 3, a resolver, a mi juicio, a favor de cualquiera de los otros apartados[7], de modo que únicamente los accesos a datos que no formaban parte de las categorías de datos contenidas en los mismos hallaban protección a través del artículo 197.3[8].

---

[5] Afirma CARRASCO ANDRINO que es simplemente el distinto carácter de los datos la nota que impide la aplicación del apartado 2 y no la existencia de un elemento subjetivo dirigido a causar un perjuicio, tal y como se ha manifestado por una parte de la doctrina al diferenciar ambos apartados. No obstante, en mi opinión, la conducta típica no es la misma en el apartado 1, idea que también deberá tomarse en consideración. Véase Sección 1ª del Capítulo IV. CARRASCO ANDRINO, 2010: 251.

[6] DE LA MATA BARRANCO y HERNÁNDEZ DÍAZ, 2010: 177.

[7] Concretamente, a mi juicio, los criterios en la resolución de los distintos conflictos:

a) Principio de especialidad: Aplicando esta idea al artículo 197, se producirá un concurso de normas a resolver en virtud del principio de especialidad cuando se produzca un acceso a datos reservados de carácter personal del apartado 2 o un acceso o apoderamiento de datos del núcleo duro de la intimidad del apartado 6. En tales supuestos, la aplicación de estos apartados primará sobre la del apartado 3 por tratarse de preceptos más específicos con motivo del objeto material.

b) Principio de subsidiariedad: Se aplicará en el artículo 197 cuando el conflicto tenga lugar en relación con la acción típica; así cuando se trate de un mero acceso a y no de un apoderamiento de correos electrónicos, documentos electrónicos o efectos personales del apartado 1, el hecho se reconducirá al apartado 3 en tanto primero habrá que averiguar si la efectiva intención del sujeto era apoderarse de los datos y no solo acceder a ellos.

c) Principio de absorción o consunción: En el artículo 197, cuando se produzca un apoderamiento de correos electrónicos, documentos electrónicos o efectos personales del apartado 1 o de datos reservados de carácter personal del apartado 2.

En cambio, considero que no existirá concurso:

d.1) Si se produce un acceso a datos del apartado 1, sin apoderamiento, entonces no existirá concurso sino que directamente pasará a aplicarse el apartado 3.

d.2) Si se produce apoderamiento de datos no comprendidos en el apartado 1, 2 y 6, entonces se aplicará el apartado 3 sin concurso.

Sobre concurso de normas véase CASTELLÓ NICAS, 2000: 14-17, 116-181. ESCUCHURI AISA, 2004. GARCÍA ALBERO, 1995: 321-424. GARCÍAS PLANAS, 1989: 109-110. VIVES ANTÓN, 1981: 8.

[8] Por todos, CHOCLÁN MONTALVO, 2006: 94.

El apartado 3 se configuraba, en consecuencia, como un tipo residual, esto es, un cajón de sastre al amparo del cual castigar todas las conductas contra la intimidad que no era posible sancionar en aplicación de los demás apartados[9]. Por este motivo, tras una primera exposición sistemática del mismo en el contexto del artículo 197, resultaba necesario efectuar una delimitación más precisa de los datos que se tutelaban en él. Para ello, debían seguirse los siguientes pasos:

> a) En primer lugar, debía fijarse qué es lo protegido en cada uno de los apartados del artículo 197, determinándose con exactitud qué eran datos contenidos en efectos personales, datos de las telecomunicaciones, datos personales automatizados y datos personales especialmente protegidos.
>
> b) Una vez establecida la premisa anterior, podía delimitarse con precisión cuáles eran los concretos datos protegidos en cada uno de los párrafos del artículo 197 y, con ello, conocer las lagunas existentes a lo largo del articulado del precepto antes de la introducción del apartado 3 por parte de la Ley Orgánica 5/2010, de 22 de junio.

Las operaciones reseñadas debían conducir, finalmente, a llenar de contenido el introducido apartado 3. Por esta razón, dedicaré las próximas páginas de esta parte del capítulo a analizar con mayor profundidad el objeto material del delito de las conductas previstas en cada uno de los párrafos de dicho precepto con el propósito de determinar las lagunas jurídicas susceptibles de ser halladas en ellos y, gracias a lo anterior, establecer su conexión con el nuevo apartado determinando con exactitud su ámbito aplicativo.

---

[9] Así, por ejemplo, la Sentencia del Tribunal Supremo 40/2016, de 3 de febrero, que castiga por el apartado 3 y no el 2 el acceso por parte del exmarido al historial clínico de su ex-mujer sin intención de causarle un perjuicio (véase F. J. 2º).

II. LOS DATOS INFORMÁTICOS DEL ARTÍCULO 197.1

El apartado 1 del artículo 197 hace referencia a papeles, cartas, mensajes de correo electrónico o cualesquiera otros documentos o efectos personales[10], un conjunto heterogéneo de elementos de naturaleza múltiple y variada[11] que comparten la característica común de consistir en soportes[12], físicos o lógicos, con capacidad para incorporar o proyectar aspectos que afectan a la intimidad de la persona[13]. La colisión de este apartado con el introducido apartado 3 se producía en relación con los soportes lógicos (susceptibles de incorporar datos informáticos) por lo que analizaré únicamente los correos electrónicos, los documentos electrónicos y, por último, los efectos personales, por integrar éstos una cláusula de cierre abierta susceptible de dar cabida a otros soportes informáticos.

---

[10] En su origen, antes de la generalización de la informática, el precepto únicamente hacía referencia a papeles y cartas. Posteriormente se incluyó la referencia a correos electrónicos, documentos y efectos personales con motivo de su adecuación a las novedades técnicas en este sector. Afirma ROMEO CASABONA que los dos últimos objetos constituyen soluciones de técnica legislativa para incluir cláusulas o recursos genéricos de recogida o de escoba de cualquier soporte idóneo para contener cualesquiera aspectos relativos a la intimidad de alguna persona. La doctrina se plantea, de hecho, si es necesario mantener la referencia a dichos elementos tras la introducción con el Código penal de 1995 del documento como objeto material del delito. ROMEO CASABONA, 2004b: 81. ROMEO CASABONA, 2004a: 726. RUEDA MARTÍN, 2004: 43. SEGRELLES DE ARENAZA, 1996: 275.

[11] ROMEO CASABONA, 2004b: 78. ROMEO CASABONA, 2004a: 726.

[12] Cabe distinguir entre el soporte de la información y la información en sí misma. Así pues, el objeto de la intimidad es la información que tiene un carácter inmaterial, mientras que el soporte que la contiene tiene carácter material o físico. En este sentido, existe la posibilidad que la información sea separable del objeto que la contiene así como puede también suceder que ambos, información y objeto, no sean disociables. En el primer caso, el sujeto se apoderará de la información, mientras que en el segundo conocerá la intimidad al mismo tiempo que se apodera del objeto. Es por ello que la doctrina se refiere en general a la proyección espacial de la intimidad, que no solo queda acotada al conocimiento de datos íntimos sino que también se materializa en los objetos personales sobre los que ésta puede quedar plasmada o proyectada. SEGRELLES DE ARENAZA, 2000: 275.

[13] CARRASCO ANDRINO, 2011: 762. GONZÁLEZ RUS, 2011a: 304. MORALES PRATS, 2008: 455. ROMEO CASABONA, 2004b: 78. ROMEO CASABONA, 2004a: 726. TOMÁS - VALIENTE LANUZA, 2010: 795.

El principal conflicto se planteaba especialmente con los mensajes de correo electrónico, respecto de los cuales ni el Código penal ni la normativa extrapenal proporciona una definición de lo que debe entenderse como tal[14]. En el ámbito de los delitos contra la intimidad, el concepto de mensaje de correo electrónico se aproxima a la noción de carta aunque con ciertas diferencias derivadas de las posibilidades técnicas que este medio de comunicación ofrece[15]. A tal efecto, me parece adecuado trasladar aquí las palabras de ROMEO CASABONA[16] cuando entiende que, desde una perspectiva jurídico-penal, correo electrónico es cualquier modalidad de comunicación de carácter personal que incorpore texto, voz, sonido o imagen y que se sirva de las redes telemáticas como tecnología de transmisión y de los sistemas informáticos (ordenadores y el software o sistema lógico correspondiente) como instrumentos de remisión y de recepción

---

[14] El hecho de que no exista en nuestro Derecho nacional un concepto legal de correo electrónico es un hecho totalmente imputable al legislador, pues el artículo 2.h) de la Directiva 2002/58/CE recoge la siguiente definición: *[t]odo mensaje de texto, voz, sonido o imagen enviado a través de una red de comunicaciones pública que pueda almacenarse en la red o en el equipo terminal del receptor hasta que pueda accederse al mismo*, que no ha sido incorporada el Derecho español en la transposición principal de dicha norma a través del Real Decreto Ley 13/2012. ROMEO CASABONA afirma que esta definición no puede ser aceptada debido a que considera que es al mismo tiempo demasiado restrictiva y demasiado amplia, ello debido a que, por una parte, no puede restringirse el concepto de correo electrónico a aquellos correos que sean enviados únicamente a través de una red pública, pero, por otra, sólo se protegen en el ámbito penal las comunicaciones electrónicas de carácter personal. ROMEO CASABONA, 2004b: 80. ROMEO CASABONA, 2004a: 726.

[15] ROMEO CASABONA, 2004b: 79. ROMEO CASABONA, 2004a: 726.

[16] No es ésta la única definición de correo electrónico propuesta en esta rama del Derecho. Partiendo de una definición amplia del mismo FERNÁNDEZ TERUELO entiende como tal cualquier fórmula que posibilite la comunicación entre sujetos a través de la Red, ya se trate de texto, imagen, audio, vídeo o de un programa de mensajería instantánea o software similar. En un sentido igualmente amplio, GONZÁLEZ RUS afirma que constituyen ficheros informatizados enviados o recibidos por vía telefónica o mediante redes de transmisión de datos. ORTS BERENGUER y ROIG TORRES hacen referencia a señales codificadas que funcionan a través de un ordenador. Parece, pues, desprenderse de la doctrina la voluntad de establecer un concepto extremadamente abierto de correo electrónico que permita englobar cualquier forma de comunicación entre particulares. FERNÁNDEZ TERUELO, 2007: 125. GONZÁLEZ RUS, 2011b: 306. ORTS BERENGUER y ROIG TORRES, 2001: 24.

entre dos o más comunicantes y, en su caso, de almacenamiento de los mensajes[17].

Cierto sector de la doctrina entiende que deben configurar el objeto material de este delito solo los mensajes de correo electrónico impresos en papel[18], puesto que para la consumación de la acción de apoderamiento interpretan como necesaria la existencia de un desplazamiento físico del mensaje, negando que ésta pueda producirse a través de lo que usualmente se conoce como apoderamiento virtual, esto es, la captación intelectual de la información a través de la mera lectura del mensaje, conducta que, a su vez, subsumen en la modalidad de interceptación de las telecomunicaciones. Totalmente en contra de esta tesis se manifiestan algunos autores, que consideran ambos supuestos incardinables en el tipo[19].

A mi parecer, resulta más acertada la opinión de quienes defienden una posición intermedia entre ambas teorías, ya que, a mi juicio, el apoderamiento puede producirse tanto de forma física como virtual, pero no en el sentido de que el desplazamiento signifique impresión física del mensaje ni tampoco en el de que el apoderamiento cognitivo implique meramente acceso intelectual. Así, pienso que:

> a) Una vez impreso, el mensaje se convierte en un papel o un documento no informático y como tal debería, en este caso, ser tratado[20].

---

[17] ROMEO CASABONA, 2004b: 80. ROMEO CASABONA, 2004a: 726.

[18] BOLEA BARDÓN, 2011: 464. MATA Y MARTÍN, 2001b: 128. MATA Y MARTÍN, 2006: 224. MORALES PRATS, 2011: 455. OLMO FERNÁNDEZ-DELGADO, 2009: 115.

[19] CARRASCO ANDRINO, 2011: 762. DAVARA RODRÍGUEZ, 2007: 370. FERNÁNDEZ TERUELO, 2007: 123. GONZÁLEZ RUS, 2011a: 306. ROMEO CASABONA, 2004c: 91.

[20] MORANT VIDAL, 2003: 61. OLMO FERNÁNDEZ-DELGADO, 2009: 115. DE LA MATA BARRANCO y HERNÁNDEZ DÍAZ, 2010: 176.

b) La conducta de apoderamiento tendrá lugar solo cuando se haya producido la recepción del mensaje en el sistema del destinatario[21], mientras que la interceptación se producirá entretanto tiene lugar el proceso de comunicación, esto es, en el periodo que va desde su emisión hasta su recepción, pero nunca cuando ya ha llegado a su destino[22].

c) El apoderamiento virtual del mensaje no supone su mera captación intelectual o cognoscitiva, sino que es necesaria la realización de una acción física dirigida a la obtención del mismo en el sentido de su desplazamiento por copia o traslación a otro dispositivo electrónico (desplazamiento virtual)[23].

---

[21] La protección se extiende no sólo al propio contenido de la comunicación -datos de contenido-, sino también a los datos de tráfico, esto es, aquellos datos que ofrecen información sobre las circunstancias en que se ha producido la misma, afectando, así, de modo directo o indirecto, a la intimidad. También a lo que se ha denominado datos mixtos, que si bien forman parte integrante del contenido de al comunicación, tienen una función de datos de tráfico. Ésta es, de hecho, la posición adoptada por la Fiscalía General del Estado en la Consulta 1/1999, de 22 de enero, sobre tratamiento automatizado de datos personales en el ámbito de las telecomunicaciones. FRÍGOLS I BRINES, 2010: 45. GARCÍA GARCÍA, 2003: 293. LLORIA GARCÍA, 2010: 177.

[22] Será interceptación conforme a esta idea la desviación del correo hacia una máquina controlada por el sujeto activo durante el periodo de transmisión o la obtención y posterior cambio de la contraseña de la dirección de correo electrónico del sujeto pasivo, impidiendo con ello el acceso por parte de éste. En contra se manifiesta ROMEO CASABONA para quien apoderamiento supone una traslación-privación del dominio, mientras que la interceptación implica una intromisión cognoscitiva en comunicación ajenas. FERNÁNDEZ TERUELO, 2007: 124. ORTS BERENGUER y ROIG TORRES, 2001: 25. A favor, FERNÁNDEZ TERUELO, 2007: 124. ROMEO CASABONA, 2004c: 88 y 95.

[23] JAREÑO LEAL afirma que el conocimiento virtual o captación intelectual del mensaje no puede equipararse a efectos típicos al concepto de apoderamiento, pues la mera idea de conocer no puede ser suficiente para integrar el injusto penal. Así pues, considera que no existe delito cuando alguien lee un correo de otro abierto en una pantalla del ordenador, de la misma forma que tampoco existirá cuando se lee una carta abierta dejada sobre la mesa. La autora pone el acento para confirmar la existencia de apoderamiento en el quebrantamiento de algún tipo de reserva para llegar al mensaje, entendiendo que el quebrantamiento de esta reserva y, con ello, el propio apoderamiento puede producirse de manera virtual, por ejemplo, mediante la obtención subrepticia de la clave de acceso. JAREÑO LEAL, 2008: 46. A favor, MATA Y MARTÍN, 2001b: 128. En contra, GONZÁLEZ RUS, 2011a: 306.

El artículo 197 no hace alusión específicamente al documento electrónico como objeto material del delito[24], aunque acertadamente la doctrina lo entiende englobado en la expresión cualesquiera otros documentos[25]. Tampoco se recoge en el Código penal una definición de este tipo de documento, si bien éste resulta perfectamente encuadrable en el concepto general de documento del artículo 26[26], que lo caracteriza como todo soporte material que exprese o incorpore datos, hechos o narraciones con eficacia probatoria o cualquier otro tipo de relevancia jurídica, noción ésta muy amplia,

---

[24] Ello contrasta con otros tipos penales como el artículo 264.1 y, especialmente, con su tipo homólogo en el ámbito del secreto de empresa, esto es, el artículo 278.1, que tipifica el descubrimiento y revelación de secretos de empresa y, a tal efecto, reza *[e]l 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.* No obstante, la literatura penal considera que aunque ambos preceptos tienen una diferente redacción, en realidad el objeto material es el mismo, siendo la única diferencia existente entre ambos el bien jurídico protegido y la pena, cuyo mínimo es superior en el caso del delito de revelación de secretos de empresa. Al respecto me parece adecuada la crítica de BACIGALUPO ZAPATER cuando puntualiza que ninguna de estas diferencias tiene un fundamento evidente y el legislador ha omitido explicar qué razones determinaron su decisión, sobre todo, por qué razón el apoderamiento de los datos de una persona fisica que no opera como una empresa, puede ser menos punible que el que perjudique a una empresa. BACIGALUPO ZAPATER, 2002: 10. Pone también de manifiesto esta circunstancia GONZÁLEZ RUS, 2011a: 306.

[25] Afirma RUIZ MARCO que la subsunción del documento electrónico se ha visto forzada por la introducción en el tenor literal del precepto de la referencia expresa al correo electrónico, hecho que, según el autor, constituye una muestra del intento de actualización de la redacción típica a la realidad tecnológica, denotando la preocupación del legislador ante los ataques a la intimidad por medios informáticos, y que, además, supone el condicionamiento de la acción de apoderamiento a los mismos. Así pues, la doctrina civilista engloba el correo electrónico dentro del concepto de documento electrónico. RUIZ MARCO, 1999: 168.

[26] BACIGALUPO ZAPATER, 2002: 13.

aplicable a todas las infracciones relacionadas con la protección de algún aspecto de éste[27].

Como puede observarse, la noción de documento en el ámbito penal se centra en el aspecto físico del mismo[28], esto es, en tanto el soporte material que contiene la información[29]. Éste no debe confundirse, sin embargo, con su contenido: la intimidad[30], la cual

---

[27] Señala BACIGALUPO ZAPATER que la creación electrónica de documentos no ha variado el concepto de documento en sí mismo, sino las maneras en las que se llevaban a cabo las funciones tradicionales de éste, básicamente el tipo de soporte en el cuál se perpetúa la declaración de voluntad en el que se documenta, la forma de garantizar la imputación del contenido, la declaración a quien la realizó y la prueba de la autenticidad mediante una certificación de determinados signos. Sin embargo, tales funciones son las mismas que las reconocidas hasta ahora en la doctrina y en la jurisprudencia. Según el autor tales ideas vienen avaladas, además, por el artículo 3.1 del Real Decreto Ley 14/1999, referido a la Posición Común de la UE de 22 de abril de 1999, que establece que la firma electrónica avanzada, siempre que esté basada en un certificado reconocido y que haya sido producida por un dispositivo seguro de creación de firma, tendrá, respecto de los datos consignados en forma electrónica, el mismo valor jurídico que la firma manuscrita en relación con los consignados en papel y será admisible como prueba en juicio, valorándose ésta según los criterios de apreciación establecidos en las normas procesales, que viene a ser la transposición de Directiva CEE 99/93, de 13 de diciembre de 1999, por la que se establecen las condiciones relativas a las firmas electrónicas y a los servicios de certificación de las mismas. BACIGALUPO ZAPATER, 2002: 3-4.

[28] A este aspecto del documento electrónico hace referencia, además, la normativa extrapenal cuando establece qué debe entenderse como tal. Concretamente, el artículo 3 de la Ley 59/2003, de 19 de diciembre, de firma electrónica,lo define como la información de cualquier naturaleza en forma electrónica, archivada en un soporte electrónico según un formato determinado y susceptible de identificación y tratamiento diferenciado Así, de entre la normativa extrapenal, diversas leyes, como, por ejemplo, el artículo 49 de la Ley 16/1985, de 25 de junio, del Patrimonio Histórico Español, especifican literalmente al definir documento que éste debe estar contenido en un soporte material, añadiendo a continuación incluso informático. De ello se desprende que el legislador entiende incluidos a los soportes de los documentos electrónicos, esto es, el hardware, como soporte material susceptible de almacenar un documento informático. Para un estudio de la noción legal de documento electrónico en el ámbito español véase AIGE MUT, 2015: 63 y ss.

[29] Véase Notas precedentes (soporte vs. información).

[30] No puede compartirse tampoco la tesis propuesta por OLMO FERNÁNDEZ OLMO FERNÁNDEZ-DELGADO, 2009: 115. CARBONELL MATEU y GONZÁLEZ CUSSAC, 2010: 287.

podrá estar almacenada tanto en un soporte puramente físico como electrónico. Así, soporte material lo será tanto el papel impreso como un USB o cualquier otro elemento informático, ya que mientras que el contenido siempre será único (aspectos íntimos de la vida de una persona), el soporte podrá variar en función de las necesidades del sujeto (USB, disco duro, tarjeta de memoria flash, etc.)[31]. Tomando en consideración esta distinción entre contenido y continente, no veo inconveniente alguno en considerar como soporte susceptible de contener o plasmar la intimidad el documento de tipo electrónico[32], siempre que en él concurran las mismas características exigidas por esta rama del Derecho para ser considerado documento a efectos penales[33].

Por último, la inclusión del inciso referente a los efectos personales ha sido discutida en la doctrina. Así pues, mientras un sector apunta a su carácter ambiguo y advierte la peligrosa extensión del tipo que su interpretación puede suponer[34] al concebirlo como el cajón de sastre del apartado[35], otros autores ponen de manifiesto que

---

[31] De hecho, la doctrina mayoritaria se decanta en el ámbito civil por un concepto amplio de documento informático, en el que cabría entender englobado también el correo electrónico. DAVARA RODRÍGUEZ, 2007: 369.

[32] DAVARA RODRÍGUEZ, 2007: 369. RUIZ MARCO, 1999: 168.

[33] En general, la doctrina y jurisprudencia penal coinciden en afirmar que debe entenderse por documento todo aquel objeto que cumpla las siguientes características:

1. Materializado: debe ser un soporte o base sólida que permita una relativa permanencia y la duración en el tiempo del contenido reflejado en él. Puede tratarse de un soporte tanto físico como informático en el que el contenido puede estar fijado tanto de forma oral como escrita.

2. Comprensible: todo o parte de su contenido debe permitir conocer, hechos, personas o circunstancias.

3. Creíble: existencia de verosimilitud entre su contenido y la realidad.

4. Identificable: es preciso poder atribuir su creación a una persona determinada o determinable.

Por todos, GILI PASCUAL y MONTSERRAT SÁNCHEZ-ESCRIBANO, 2014: 70.

[34] ROMEO CASABONA, 2004b: 80. ROMEO CASABONA, 2004a: 726.

[35] OLMO FERNÁNDEZ-DELGADO, 2009: 116. CARBONELL MATEU y GONZÁLEZ CUSSAC, 2010: 327 (CD).

constituye la cláusula que convierte en innecesaria la alusión a todos los demás objetos en él mencionados[36], pues todos ellos son, en realidad, efectos personales[37]. Más acertada me parece la opinión de quienes consideran como tal cualquier artículo personal que posea un contenido de intimidad para el sujeto pasivo[38] en el sentido no de su objeto (contener datos relativos a la intimidad), sino, como indica QUERALT, de su función (ser expresivos de la intimidad no en sí mismos considerados o por ser portadores de la misma, sino por ser utilizados o atribuido su uso al titular de la intimidad)[39]. Ello implica extender la protección del artículo 197.1 a todos aquellos elementos en los que se puede proyectar la intimidad del sujeto, tanto si se trata de soportes respecto de los que ésta es susceptible de ser disociada como de aquellos casos en los que esto no es posible por tratarse de objetos que la proyectan por sí mismos[40].

A efectos de acabar de delimitar el objeto del delito, aparte de la enumeración estudiada, el apartado 1 del artículo 197 añade una nota de suma relevancia en la dicción literal del precepto, el posesivo *sus*, pues ésta reza: se apodere de sus papeles. Concretamente, la introducción del posesivo sus implica que la conducta sólo será típica si la persona cuya intimidad se ve afectada (esto es, el sujeto pasivo del delito) es también titular del soporte de apoderamiento[41]. Se

---

[36] RUEDA MARTÍN, 2004: 43.

[37] Debido a la amplitud con la que ha sido redactada dicha cláusula se afirma que dicha enumeración tiene únicamente un carácter ejemplificativo, de modo que en realidad se está protegiendo cualquier efecto personal que contenga datos que pertenezcan a la intimidad, o que por sí mismo ya denote un aspecto de la misma. SEGRELLES DE ARENAZA, 2000: 275.

[38] ROMEO CASABONA, 2004b: 80. ROMEO CASABONA, 2004a: 726.

[39] QUERALT JIMÉNEZ, 2010: 294. Siguiendo a QUERALT, JORGE BARREIRO, 1999: 114..

[40] SEGRELLES DE ARENAZA, 2000: 275.

[41] CARBONELL MATEU y GONZÁLEZ CUSSAC, 2010: 327 (CD). MORALES PRATS, 2008: 457. OLMO FERNÁNDEZ-DELGADO, 2009: 97-98. ROMEO CASABONA, 2004c: 76.. RUEDA MARTÍN, 2004: 40. RUIZ MARCO, 1999: 170. TOMÁS - VALIENTE LANUZA, 2010: 796.

exige, por tanto, una plena correspondencia entre el titular del soporte objeto de apoderamiento y el titular de los datos informáticos (doble titularidad)[42], de modo que, si los datos apoderados pertenecen a un tercero, la conducta no entra dentro del ámbito típico del apartado 1 del artículo 197[43].

Tomando en consideración todo lo anterior, el apartado 1 del artículo 197 cubre los posibles ataques informáticos a la intimidad que consistan en el apoderamiento o bien de datos informáticos contenidos en correos electrónicos o documentos electrónicos almacenados en el sistema informático del titular de los mismos, o bien de efectos personales informáticos que, aun no siendo objetos contenedores de datos informáticos sensu stricto, son expresivos en sí mismos de la intimidad de la persona. Fuera de dicho ámbito quedan todo un conjunto de supuestos de deseable punición cuya sanción quedaba garantizada a partir de 2010 al amparo del apartado 3.

---

[42] Con carácter general la doctrina admite, aunque crítica, la existencia de esta doble titularidad. Se aduce al respecto la ausencia de justificación de la reducción del ámbito típico que se atribuye a la concepción patrimonialista que presidió la configuración del injusto típico y que supone la insidiosa exclusión de hechos tales como el de la persona que, para descubrir la identidad de otro, se apodera de documentos que un tercero tiene sobre él. Advierte ROMEO CASABONA, no obstante, que si bien es cierto que la introducción del posesivo sus conduce a restringir de forma excesiva la intimidad, la cuestión no es tan sencilla de resolver, porque de no exigir la concurrencia de la referida identidad podría ocurrir que el poseedor legítimo del soporte, en el ejemplo acabado de ilustrar, incurriera en el delito, de no contar él mismo previamente a la cesión del documento a tercero con el consentimiento de la persona a la que se refiere el contenido íntimo que incorpora el soporte. Pone de relieve en este sentido el autor que llegar a este resultado sí que podría ser excesivo porque el poseedor legítimo del soporte no realiza ningún acto de apoderamiento ni descubre nada contra la voluntad del sujeto pasivo, pues ya era conocedor del contenido desde que éste le entregó -voluntariamente- el soporte. MORALES PRATS, 2008: 457. ROMEO CASABONA, 2004c: 76-77. RUEDA MARTÍN, 2004: 40. RUIZ MARCO, 1999: 170.

[43] Aunque, como se ha visto, ésta es la opinión compartida por la doctrina mayoritaria, no faltan opiniones doctrinales o resoluciones judiciales que castigan o se manifiestan a favor de la inclusión de tales supuestos. Así pues, considera punibles estos supuestos REBOLLO 2004, 455-6, así como implícitamente la SAP Zaragoza 264/2008, 3 de julio, que condena al sujeto que, habiendo sido autorizado por una conocida para acceder y grabarse archivos musicales contenidos en su teléfono móvil, accede y se guarda en su propia terminal unas fotos eróticas de una tercera persona).

Concretamente, las lagunas que el nuevo apartado venía a solventar eran las siguientes:

> **a) Accesos no calificables como apoderamiento:** puesto que el objeto material del artículo 197.3 era en cierto modo coincidente con el del apartado 1, la subsunción de la conducta en uno y otro apartado estribaba en el distinto alcance de la acción típica. En consecuencia, mientras la comisión de actos sobre dichos objetos a través de algún género de aprehensión física quedaban subsumidos en el apartado 1, se castigarían a través del apartado 3 todos aquellos comportamientos en los que no se produjera ese plus que exige la acción de apoderamiento -calificables, por tanto, como acceso-, entre otros la mera captación intelectual del contenido de un mensaje de correo electrónico, de un documento electrónico o de un efecto personal. De este modo, el apartado 3 se instituía en un tipo atenuado respecto del primer párrafo del artículo 197.
>
> **b) Apoderamiento o acceso a datos de terceros:** en la medida en que el apartado 1 del artículo 197 exigía la doble titularidad a la que se ha hecho referencia (el sujeto debía ser titular del soporte y también titular de los datos), quedarían amparados en el apartado 3 el acceso o apoderamiento de un soporte con datos pertenecientes a un tercero[44].

[44] Ello permitía también solventar los problemas planteados en la nota 56.

III. LOS DATOS INFORMÁTICOS DEL ARTÍCULO 197.2

El apartado 2 del artículo 197 recoge como objeto material los 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.

Tomando en consideración la ubicación sistemática del precepto y la propia sistematización del Código penal conforme al bien jurídico protegido, aun afirmando a priori que este apartado tutela el habeas data o poder de control y disposición sobre los datos personales, —que en sede de interpretación constitucional abarca cualquier dato que guarde relación con la personalidad, esto es, todos aquellos que identifiquen o permitan la identificación de la persona o que sirvan para cualquier otra utilidad que en determinadas circunstancias constituyan una amenaza para el individuo—, en el ámbito penal, la vulneración de este derecho queda circunscrita únicamente a aquellos supuestos en los que se vea comprometida la intimidad[45] (o lo que cierto sector de la doctrina ha denominado intimidad informática)[46]. Así pues, por medio de este apartado no se tutelan todos los datos, sino únicamente aquellos que cumplen cuatro condiciones: tratarse de datos de carácter personal o familiar, ser de otro, ser reservados y, por último, estar contenidos en ficheros públicos o privados. Véase, a continuación, cada una de estas características con más detenimiento:

---

[45] La doctrina entiende al respecto clave de este precepto se halla no tanto en vulnerar la intimidad como en acceder ilegítimamente a ella, hecho que según la autora supone una derivación hacia una concepción formal de la intimidad como bien jurídico protegido, ya que a la concepción negativa del derecho a la intimidad como facultad de exclusión de terceros, se ha visto completada por este aspecto positivo en tanto poder de control y disposición sobre la información. JAREÑO LEAL, 1999: 15.. Ver también, entre otros, MARCHENA GÓMEZ, 2001: 1099.. ORTS BERENGUER y ROIG TORRES, 2001: 23..

[46] SOTO NIETO defiende que el elemento del perjuicio que prevé este tipo como factor tendencial de la parte subjetiva de la conducta se culmina con el menoscabo del propio bien jurídico, pues la afectación de la intimidad según el autor ya produce un perjuicio al sujeto pasivo. SOTO NIETO, 2004: 3 de 6.. También en SOTO NIETO, 2001: 3 y 4 de 4..

Definir dato personal es bastante sencillo puesto que, de acuerdo con el artículo 3 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal[47], se trata de cualquier información concerniente a personas físicas identificadas o identificables. En el ámbito penal se exige, además, que con ello se vea comprometida la intimidad, lo que no significa ceñir la tutela solo a los más sensibles, a los que ya ofrece protección, agravada, el artículo 197.5[48]. Aunque lo anterior es tarea fácil, resulta complejo diferenciar este dato del familiar[49], el cual, en realidad, no es más que una subespecie de éste vinculado a lo que constitucionalmente se

---

[47] Esta norma constituye la transposición del artículo 2 a) la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (modificada por el Reglamento (CE) n° 1882/2003 del Parlamento Europeo y del Consejo de 29 de septiembre de 2003), que establece que dato personal es toda información sobre una persona física identificada o identificable (el "interesado"); se considerará identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un número de identificación o uno o varios elementos específicos, característicos de su identidad física, fisiológica, psíquica, económico, cultural o social.

[48] Quedan fuera del ámbito de protección del precepto, por tanto, todos aquellos datos que han sido sometidos a un procedimiento de disociación que impida su vinculación a o la identificación de la persona concreta que lo ha revelado, dejando de tener, por tanto, carácter personal. FERNÁNDEZ TERUELO, 2007: 136.. JORGE BARREIRO y RODRÍGUEZ MOURULLO, 1997: 254.. MORALES PRATS, 2011: 472-473.. ORTS BERENGUER y ROIG TORRES, 2001: 32-33.. ROMEO CASABONA, 2004b: 48.. E, igualmente, en ROMEO CASABONA, 2003: 534.. STS 11 junio 2004

[49] Nótese que ambas notas, que el Código penal predica de los datos personales, en realidad, en el artículo 18.1 y .4 del Texto Constitucional aparecen vinculadas al derecho a la intimidad y no a los datos personales. Igualmente, el desarrollo jurisprudencial del Tribunal Constitucional tampoco ha cimentado su construcción del derecho a la protección de datos sobre estas dos características. En mi opinión, este lapsus legislativo se debió a la aprobación del Código penal en el momento en que era opinión mayoritaria en la doctrina que el único derecho del que se podían derivar ataques por parte de la informática es el derecho a la intimidad. Esta cuestión llama también la atención de ROMEO CASABONA, quien opina que no parece que constituya trastorno insuperable tal expansión del tipo. No considero, como el autor, que esta afirmación constituya una ampliación extensiva del tipo, sino meramente una circunscripción restrictiva del bien jurídico. ROMEO CASABONA, 2004b: 47.. ROMEO CASABONA, 2003: 533.. RUEDA MARTÍN, 2004: 71..

llama núcleo familiar, ello, a mi juicio, con independencia del grado de parentesco existente entre las personas convivientes[50].

Sencillo resulta, también, determinar qué son datos de otro, pues todo lo que no es propio y tiene dueño es de otro, siendo que el objeto material del delito se integra esta vez, a diferencia de lo que sucedía en el apartado 1, por cualquier dato que, reuniendo las demás características, sea ajeno al sujeto activo.

A los efectos de determinar qué debe entenderse por dato de carácter reservado[51], pueden observarse en la doctrina dos posturas:

a) Posturas amplias: cierto sector doctrinal es partidario de extender el espectro aplicativo de este apartado lo máximo posible y, con tal finalidad, han propuesto una ampliación tan extensiva del tipo que contraviene el propio sentido y tenor de la Ley:

a.1) Algunos autores se manifiestan a favor de entender amparado en la protección penal cualquier dato personal, con independencia de su carácter íntimo, afirmación que, a mi juicio, socava el bien jurídico[52].

a.2) Otros consideran que todos los datos personales una vez introducidos en un fichero automatizado son sensibles y, por tanto, expresivos de la intimidad, porque un dato en principio inocuo pero registrado en un fichero automatizado puede ser objeto de

---

[50] Se pregunta sobre ello SEGRELLES DE ARENAZA, 2000: 286..

[51] Como señala MATA y MARTÍN existe cierto desconcierto en la doctrina acerca de la determinación de qué debe entenderse por dato reservado, fruto de la discordancia en este punto entre el Código penal y la propia Ley Orgánica de Protección de Datos. Como puede observarse de la lectura de este apartado puesto en relación con el artículo 7 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, el concepto empleado por el Código penal para referirse a los datos objeto de protección es distinto al que emplea la propia Ley de Protección de Datos, que hace referencia a datos especialmente protegidos. Véase MATA Y MARTÍN, 2001a: 133..

[52] GÓMEZ NAVAJAS, 2005: 129..

manipulación y/o permitir obtener información por inferencia con motivo de las diversas posibilidades que dichos sistemas permiten[53].

a.3) Finalmente, se defiende que la tutela penal se extiende a aquellos datos que afecten a un ámbito más amplio que la intimidad como es la privacidad del sujeto, con independencia de si los datos se encuentran o no incorporados en el sistema informático[54].

b) Postura restrictiva: Las tesis anteriores no resultan aceptables conforme al punto de vista defendido en el presente estudio[55]. Ciertamente me parece, siguiendo a un acreditado sector de la doctrina, adecuado adoptar una posición más restringida cimentada en la idea de que el concepto de dato reservado se sitúa en un rango intermedio entre la noción de dato personal y los datos del artículo 197.5[56]. Ello se justifica en dos argumentos:

b.1) Descriptivo-terminológico: reservado es lo que no es público, esto es, aquello a lo que no se tiene libre

---

[53] Sin embargo, al respecto señala MARTÍN-CASALLO LÓPEZ que la acumulación indiscriminada de datos personales, que denomina amontonamiento de datos personales sin criterios de estructuración o clasificación, no viene a integrar la órbita del precepto por ser un acto que carece de la suficiente entidad para considerarlo un ataque contra el bien jurídico protegido. En cambio, sí que se hallarían protegidos por el mismo los datos que figuran en Internet. MARTÍN-CASALLO LÓPEZ, 2000: 21.. MORALES PRATS, 2011: 467 y 468..

[54] MORALES PRATS, 2011: 468..

[55] Véase, para ello, Capítulo III.

[56] A favor, TOMÁS - VALIENTE LANUZA, 2010: 800. Haciendo referencia también a una concepción más restringida: la intimidad más estricta ORTS BERENGUER y ROIG TORRES, 2001: 33..

acceso por parte de cualquiera y se ha restringido o limitado a terceros[57].

b.2) Legal: por una parte, los datos reservados deben considerarse como un subgénero de datos personales, definidos éstos por el artículo 3 de la Ley Orgánica de Protección de Datos de Carácter Personal, antes transcrito, como cualquier información concerniente a personas físicas identificadas o identificables; y, por otra, ello con exclusión de los denominados datos personales especialmente protegidos, pues éstos ya constituyen el objeto de la agravación del apartado 5.

La última característica que se predica de los datos es que se encuentren registrados en ficheros o soportes informáticos, electrónicos o telemáticos, o en cualquier otro tipo de archivo o registro público o privado. La interpretación de este inciso ha sido especialmente conflictiva, ya que mientras por una parte la doctrina se interpreta que los datos deben hallarse registrados en ficheros o registros en el sentido de conjuntos organizados de información[58],

---

[57] Entiende acertadamente la doctrina que dicha interpretación restrictiva goza de importantes ventajas (permitiría explicar mejor, por ejemplo, la tipificación individualizada del mero acceso a los datos aunque no se hayan utilizado ni alterado), amén de resultar coherente con el principio de intervención mínima y el carácter subsidiario de la protección penal frente a la administrativa, en la línea de evitar condenas con penas muy elevadas que se antojan de escasa trascendencia. SEGRELLES DE ARENAZA, 2000: 2000. MATA Y MARTÍN, 2001b: 134. RUIZ MARCO 198. ORTS BERENGUER y ROIG TORRES, 2001: 32-33. 32-33, DOVAL PAÍS y JAREÑO LEAL, 2000. ROMEO 2004. TOMÁS Y VALIENTE 801 FERNÁNDEZ TERUELO, 2007: 136.. RUEDA MARTÍN, 2004: 71.. RUEDA MARTÍN, 2004: 71..

[58] La doctrina que defiende esta tesis se ampara en la definición propuesta por el artículo 3 b) de la Ley Orgánica de Protección de datos, que define fichero o soporte informático como todo conjunto organizado de datos de carácter personal, cualquiera que fuere la forma o modalidad de creación, almacenamiento, organización y acceso. Lo cierto es que el apartado 2 del artículo 197 utiliza el verbo registrar en lugar de almacenar y hace referencia a archivos o registros de carácter público o privado, lo que me conduce a inclinarme a favor de la exigencia de que los datos se hallen recopilados de algún modo. Sentencia Audiencia Provincial de Ciudad Real de 23 de abril de 2001 HUERTA TOCILDO y ANDRÉS DOMÍNGUEZ, 2002: 57.. MORALES PRATS, 2011: 472-473.. TOMÁS - VALIENTE LANUZA, 2010: 801.. RUEDA MARTÍN, 2004: 76..

otros autores consideran que se trata de una cláusula general que permite englobar cualquier soporte idóneo para contener datos informáticos, ejemplificando como tales incluso el disco duro del ordenador[59]. Defender la primera tesis, que me parece la más acertada, suponía trasladar todas las conductas de apoderamiento o acceso a datos no registrados a la órbita del apartado 3, hecho que abarcaría también algunos de los comportamientos vinculados al proceso de tratamiento informático de datos como la creación de ficheros automatizados o la recogida de datos personales[60].

En último lugar, es necesario poner en relación este apartado con los restantes párrafos del artículo 197. Para FERNÁNDEZ TERUELO su función es cubrir las lagunas del apartado 1 del artículo 197[61], algo que, efectivamente, se produce en el sentido de aplicarse a datos informáticos relativos a la intimidad que no se encuentran en poder del sujeto pasivo tal y como sucede en el párrafo 1. Sin embargo, nuevamente se observaban lagunas que permitían la aplicación del apartado 3. Tales supuestos son los siguientes:

---

[59] Afirma FERNÁNDEZ TERUELO que el propio artículo 2 de la Ley Orgánica de protección de Datos hace referencia a datos de carácter personal registrados en soporte físico, que los haga susceptibles de tratamiento y a toda modalidad de uso posterior de estos datos por los sectores público y privado. Caben, por tanto, en nuestro ámbito de estudio todo tipo de soporte físico o virtual, que posibilite mediante la conexión a la red el acceso a los datos. RUIZ MARCO, 1999: 200.. CARBONELL MATEU y GONZÁLEZ CUSSAC, 2010: CD.. FERNÁNDEZ TERUELO, 2007: 136.. ORTS BERENGUER y ROIG TORRES, 2001: 33..

[60] Muy ilustrativa resulta al respecto la Sentencia de la Audiencia Provincial de Guipúzcoa de 21 de marzo de 2000, que establece que: el Código ha optado por reducir el ámbito de los ilícitos penales a las conductas de apoderamiento, utilización, modificación, acceso ilegítimo, alteración y cesión de los datos registrados, es decir, que la protección penal no abarca todo el proceso del tratamiento informatizado de los datos, se limita a la tutela de los datos ya registrados, excluyendo las fases de creación de los ficheros automatizados y de recogida de los datos personales, que se reconducen al ámbito de la responsabilidad administrativa. Así pues, se trata de datos informáticos contenidos en una parte muy concreta de los sistemas informáticos, concretamente en archivos y registros públicos o privados.

[61] FERNÁNDEZ TERUELO, 2007: 136..

a) Acceso a datos que no sean personales o familiares: cuestión sumamente interesante es la de si, además de entender englobados en el apartado 3 los datos personales que no tenían cabida en el apartado 2, también debía ser subsumible el acceso a datos que no tuvieran este carácter. En mi opinión, aunque no deben excluirse de inicio ningún tipo de datos, resultaba difícil encontrar un dato que no fuera personal y contuviera o fuera reflejo de la intimidad de la persona, pues un dato que no sirve para poder identificar a una persona tampoco puede ser reflejo de su intimidad.

b) Acceso a datos personales que no sean reservados: en la medida en que el artículo 197.2 protege el acceso a datos personales de carácter reservado y que, habiendo optado por la concepción restrictiva, esto supone que no resultan protegidos todos los datos personales, sino únicamente aquellos en relación con los que el sujeto ha restringido su conocimiento a un número limitado de personas, todos aquellos datos personales en los que no concurra la condición de reservados quedaban desde 2010 al amparo del apartado 3.

c) Acceso a datos que no sean registrados: en la medida en que los datos a los que se refiere el apartado 2 deben estar registrados, esto es, integrados en un conjunto organizado de información, todas las conductas cuyo objeto son los datos personales que no ostentaran tal condición (como, por ejemplo, aquellas a las que ya se ha hecho alusión en la página anterior) serían castigadas al amparo del apartado 3.

IV. LOS DATOS ESPECIALMENTE SENSIBLES DEL ARTÍCULO 197.5 (ACTUAL .6)

El artículo 197.5, que opera como subtipo cualificado en relación con los apartados anteriores, contiene dos agravaciones: una por razón del objeto material, esto es, la especial naturaleza de los datos sobre los que recae la infracción penal (ideología, religión, creencias, salud, origen racial y vida sexual); y otra en atención a las particulares características del sujeto pasivo (menores o incapaces).

La especial cualificación de las conductas por razón del objeto material, que es la que aquí interesa, tiene como fundamento otorgar reforzar la protección del ámbito más básico de la intimidad[62] debido, principalmente, al mayor contenido de injusto que implica su afectación[63] aunque también por razones de política-criminal[64]. Se trata de datos e informaciones, informáticos o no[65], que se integran por lo que el artículo 7 de la Ley Orgánica de Protección de Datos

---

[62] También se ha hecho referencia en una opinión excesivamente amplia al núcleo duro de la intimidad informática (RUIZ MARCO) o, en una posición extremadamente amplia, al núcleo duro de la privacy (MORALES PRATS, ALONSO DE ESCAMILLA) ROMEO CASABONA, 2004c: 155.. MORALES PRATS, 2008: 476-477.. ALONSO DE ESCAMILLA, 2013: 221.. Sentencias 1461/2001, de 11 de julio, 1444/2004, de 10 de diciembre. Sentencia de la Audiencia Provincial de Tarragona de 4 de febrero de 2002, Sentencia de la Audiencia Provincial de Madrid de 15 de abril de 1999, Sentencia de la Audiencia Provincial de Pontevedra de 18 de mayo de 2001 SEGRELLES DE ARENAZA, 1996: 204-295.. RUIZ MARCO, 1999: 212..

[63] CARRASCO ANDRINO, 2011: 762. ORTS BERENGUER y ROIG TORRES, 2001: 44.

[64] MORALES PRATS, 2008: 476-477..

[65] Como muy bien indica MORALES PRATS, sorprende el hecho de que se afirme que puedan ser objeto de informatización o automatización ciertos tipos de datos como el origen racial, las creencias o la vida sexual de las personas, pues en el artículo 6 del Convenio del Consejo de Europa de 1981 se afirma que tales datos en principio no son informatizables. MORALES PRATS, 2008: 476-477..

denomina datos especialmente protegidos[66] a causa de su extrema sensibilidad: ideología, religión, creencias, salud, origen racial y vida sexual.

La realización de las conductas previstas en cualquiera de los apartados anteriores del artículo 197 contra cualquiera de las tipologías de datos enunciadas en el apartado 5 suponden la aplicación preferente de éste sobre los demás apartados, al producirse un concurso de normas a resolver en virtud de la regla primera del artículo 8 del Código penal, relativa al principio de especialidad, en atención al carácter más restringido de los datos contenidos en él. Ello también se hacía extensivo tras la introducción del apartado 3 a la nueva conducta prevista en él cuando se tratarse

[66] Concretamente, el artículo 7 de la Ley Orgánica de Protección de datos, rubricado Datos especialmente protegidos, hace referencia en su apartado 1 a la ideología, religión o creencias, en el segundo a los datos de carácter personal que revelen la ideología, afiliación sindical, religión y creencias, en el tercero [l]os datos de carácter personal relativos al origen racial, a la salud y a la vida sexual, en el cuarto a los datos de carácter personal que revelen la ideología, afiliación sindical, religión, creencias, origen racial o étnico, o vida sexual, y, finalmente, en el quinto a [l]os datos de carácter personal relativos a la comisión de infracciones penales o administrativas. Si se compara dicho precepto con el apartado 5 (hoy 6) del artículo 197 solo hace referencia a los datos relativos a la ideología, afiliación sindical, religión y creencias, al origen racial, a la salud o a la vida sexual, excluyendo, por tanto, la afiliación sindical, el origen étnico y los datos relativos a la comisión de infracciones penales.

de datos relativos a ideología[67], religión, creencias[68], salud[69], origen

[67] La Sentencia del Juzgado de lo Penal de Madrid, Sección 16ª número 531/2001, de 18 de diciembre, considera la afiliación a un partido político como el acto más elemental para identificar a una persona con una ideología concreta.

[68] Sin embargo, absuelve la criticada Sentencia de la Audiencia Provincial de Navarra de 31 de julio de 2003 en un caso de apropiación de un certificado de asistencia a un curso sobre Desarrollo Espiritual y Medianidad al considerar que no constituye una revelación detallada de ningún aspecto de los protegidos en este precepto.

[69] La Sentencia de la Audiencia Provincial de Valladolid de 14 de julio de 1998, confirmada por la Sentencia 9 de octubre del 2000, aplica el tipo agravado comentado en un supuesto de apoderamiento de datos personales, relativos al estado y condiciones de salud fisica y mental y a informes psicológicos, registrados en el fichero informático de una asociación de minusválidos. Sin embargo, el Auto de la Audiencia Provincial de Álava, Sección 2ª, de 28 de noviembre de 2005, considera típica la conducta del médico que informa de la enfermedad que padece un candidato a la policía municipal, lo que motivó la exclusión del afectado del proceso selectivo por padecer una diabetes prevista como causa excluyente. La resolución considera atípica la conducta porque se realizó en cumplimiento de la obligación deontológica de informar, con la finalidad de evitar un peligro al enfermo y terceras personas. La Sentencia de la Audiencia Provincial de Zaragoza de 19 de junio de 2002 aplicó este tipo agravado al apoderamiento por parte del cónyuge de un diario personal del sujeto pasivo en el que ésta recogía aspectos relativos a su salud física y psíquica y a su vida sexual.

racial y vida sexual[70].

[70] Como indica TOMÁS Y VALIENTE LANUZA, en el concreto caso de los datos referentes a la vida sexual, el Tribunal Supremo se muestra poco claro: en alguna sentencia propone la restricción de la agravante a la revelación de orientaciones sexuales que pudieran considerarse por algunos sectores al margen de la norma general, denegando su aplicación a casos de revelación de relaciones extramatrimoniales (STS 302/2008, de 27 de mayo Fj 3º), mientras que en otra sí lo ha aplicado a supuestos de esta última clase (STS 696/2003, de 20 de junio). TOMÁS - VALIENTE LANUZA, 2010: 805.. La Sentencia del Tribunal Supremo 1219/2004, de 10 de diciembre, Fundamento Jurídico 8 considera que las imágenes que contienen o revelan datos o aspectos de la vida sexual del denunciante afectan al núcleo duro del derecho a la intimidad. La Sentencia de la Audiencia Provincial de Toledo, Sección 1ª de 17 de octubre de 2005, considera típica la divulgación pública de los datos de filiación de un menor de edad, víctima de un delito contra la libertad sexual, que constaban en un informe forense. También se pronuncia sobre ello la Sentencia de la Audiencia Provincial de Tarragona de 4 de febrero de 2002 sobre la grabación en imágenes de carácter sexual, y las Sentencias del Tribunal Supremo de 20 de junio de 2003, de la Audiencia Provincial de Zaragoza de 19 de junio de 2002, de la Audiencia Provincial de Pontevedra de 18 de mayo de 2001 en cuanto a la grabación de conversación telefónicas a los efectos de descubrir supuestas infidelidades amorosas. También referentes a grabaciones de conversaciones telefónicas en las que se hablaba sobre datos de carácter sexual la Sentencia de la Audiencia Provincial de Zaragoza de 23 de octubre de 2001 y la Sentencia de la Audiencia Provincial de Barcelona de 24 de octubre de 2001.

V. LOS DATOS INFORMÁTICOS DEL APARTADO 3 DEL ARTÍCULO 197 CONFORME A LA REDACCIÓN DE LA LEY ORGÁNICA 5/2010, DE 22 DE JUNIO

Las páginas anteriores se han dedicado a la delimitación de los datos que se protegían en el apartado 3 del artículo 197 mediante una delineación negativa forzada por la ubicación sistemática del precepto y por la parquedad de la definición que el legislador había diseñado para determinar cuál era el objeto material del delito. La pregunta a plantear una vez encuadrado el delito de acceso ilícito en el seno del descubrimiento y revelación de secretos era si resultaba viable ofrecer un concepto legal de datos informáticos desde una perspectiva positiva.

No resultaba tarea fácil encontrar una definición que permitiera englobar todos los datos que era deseable proteger mediante el artículo 197.3 y, a la vez, posibilitara restringir su aplicación excluyendo aquellos que no lo eran. Dos eran las únicas definiciones que podían tenerse en cuenta: la recogida en la normativa supranacional y la que se establece en la § 202a (2) del Código penal alemán. Véase cada una de ellas por separado:

A) DEFINICIÓN SUPRANACIONAL DE DATO INFORMÁTICO

Podría analizarse, a continuación la definición ofrecida por la normativa supranacional, esto es, por el Convenio sobre Cibercrimen de Budapest, de 23 de noviembre de 2001, y la Directiva, 2013/40/UE, de 12 de agosto de 2013, del Parlamento Europeo y del Consejo, relativa a los ataques contra los sistemas de información y por la que se sustituye la Decisión marco 2005/222/JAI del Consejo. Recordando la definición de datos informáticos que efectúan ambas normas: *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.*

Conforme a esta definición **dato informático** sería toda aquella información que se introduce en un sistema informático y que es susceptible de tratamiento automatizado por éste. Al amparo de este concepto quedarían englobados todo género de datos que se encuentran almacenados dentro del sistema informático[71].

B) DEFINICIÓN CONTENIDA EN la § 202a (2) DEL CÓDIGO PENAL ALEMÁN

El Código penal alemán también ofrece una noción de dato informático vinculada a este delito en concreto[72]. La § 202a (2) StGb afirma que los únicos datos protegidos en el delito de espionaje de datos son aquellos que se almacenan o trasmiten en forma electrónica, magnética, o de otra manera en forma no inmediatamente perceptible[73].

---

[71] Véase también Epígrafe III.C) de la Sección 2ª de este Capítulo.

[72] a) El punto de referencia de esta definición es la Norma Din 44300 del Instituto Alemán Nacional de Normación, que define datos como estructuras de signos o funciones continuas que tienen como finalidad la representación de la información a través de convenios o acuerdos conocidos destinados a un fin de procesamiento u con cualquier otro resultado. Además, la norma distingue también entre datos analógicos y datos digitales, entendiendo los primeros como aquellos que sólo están compuestos por signos y los segundos por aquellos que están compuestos por funciones continuas. Sin embargo, la opinión mayoritaria está basada en un entendimiento amplio del concepto de datos, que incluye no solo datos con una finalidad de procesamiento sino también información sin un propósito directo de procesamiento. b) El Instituto Alemán Nacional de Normación es el órgano central para la creación de las normas nacionales de Alemania, con reconocimiento a nivel tanto nacional como internacional y europeo, y miembro del la Organización Internacional y Europea para la Normación. Su principal cometido consiste en la elaboración, adopción y reconocimiento de las normas así como hacerlas accesibles al público. El resultado de su trabajo son la elaboración de las normas DIN, que son las normas de tipo standard del Instituto Alemán Nacional de Normación que sobre tratan en una multitud de campos, en relación con sobre aspectos relacionados con la tecnología, tratando de crear una uniformidad en el ámbito informático de acuerdo con criterios objetivos. Concretamente, las Normas DIN 44300, un total de nueve, tratan de uniformizar las cuestiones jurídicas relativas a los conceptos generales, presentación de la información, las estructuras de datos, programación, construcción de sistemas informáticos digitales, de almacenamiento, el tiempo, las funciones de procesamiento y las operaciones de procesamiento. DIN, 1988: 1.. KLEIN, 1997: 35.

[73] (2) *Daten im Sinne des Absatzes 1 sind nur solche, die elektronisch, magnetisch oder sonst nicht unmittelbar wahrnehmbar gespeichert sind oder übermittelt werden.*

En general, la definición que contiene dicha Sección del Código penal alemán es muy abierta[74] y centrada en el concepto de información, siendo las únicas características que los definen: ser ajenos al sujeto activo, ser o estar siendo transmitidos o almacenados de una forma no directamente perceptible y estar protegidos[75]. Los dos últimos aspectos han sido muy criticados por la doctrina alemana, que, de hecho, atribuye un valor muy escaso a esta definición, al entender que conforme a ella no es posible identificar cuáles son los datos a los que se ofrece protección. Véanse los principales puntos objeto de crítica:

> **a) Excesiva generalidad:** En primer lugar, se aduce que se trata de una enunciación genérica que resulta aplicable a cualquier ámbito del Derecho sin que aporte nada en particular a la descripción penal del tipo, al no poderse establecer relación directa con él[76]. La razón principal para ello se centra en que la noción legal de dato no aparece claramente delimitada en la misma de una manera positiva sino únicamente a través de la limitación del concepto por medio de la exigencia de características adicionales[77]. Así pues, dentro del concepto de datos ex § 202a (2) quedan englobados

---

[74] ALTENHAIN y WIETZ, 2013: o párrafo 2.. FISCHER, 2015: página 1395 o párrafo 2.. GRAF, 2012: 181 o párrafo 12.. HILGENDORF, 2005: 1442 o párrafo 7.. HOYER, 2012: 3 o párrafo 3 (Abschnitt 15).. KARGL, 2013a: 1407 o párrafo 4. KINDHÄUSER, 2013: 1819.. HEGER, 2014: 965 o párrafo 2.. SCHÖNKE y SCHRÖDER, 2010: 1820.. TAG, 2013: 1091 o párrafo 4.. WEIDEMANN, 2010: 1307 o párrafo 4..

[75] A ello se hará referencia en el Capítulo VI.

[76] BOSCH, 2014: 1275 o párrafo 2.. KARGL, 2013b: 1407 o párrafo 4..

[77] El único aspecto positivo que la doctrina alemana concibe en la definición es su apertura a los nuevos avances de la tecnología. Parece, pues, que el legislador alemán, aún habiendo ido un paso más allá que el español al pretender positivizar el concepto de datos informáticos, en realidad ha cometido los mismos errores que éste a la hora de configurar el concepto de datos informáticos, que adolece de las mismas deficiencias que el artículo 197.3: excesiva generalidad y delimitación mediante una interpretación de carácter negativo. ALTENHAIN y WIETZ, 2013: o párrafo 2.. GRAF, 2012: 180-181 o párrafo 10.. KARGL, 2013b: 1407 o párrafo 4.. TAG, 2013: 1091 o párrafo 4..

todo tipo de datos[78] y de cualquier formato[79]. Una suerte de restricción similar a la interpretación conforme al bien jurídico es realizada por KARGL, para quien solo pueden caer en la esfera de la § 202a (2) datos con un interés legítimo para el uso y el conocimiento del propietario, o GRAF, al defender que, aunque la formulación de datos del apartado 1 habla de datos en general, debe tratarse de datos protegidos contra el espionaje[80].

b) Vinculación directa con el concepto de información: Se afirma también que la noción de dato se centra excesivamente en el concepto de información. De este modo, éste se define como una representación de la información que es susceptible de ser entendida a través de códigos definidos con independencia de esté dirigida a fines de procesamiento[81].

c) Limitación de imperceptibilidad: En último lugar, los datos en la § 202a (2) StGb son solo aquellos que sean transmitidos o almacenados de una forma no directamente perceptible, esto es, que se trate de información codificada[82] por hallarse registrados, o bien por hallarse almacenados de una forma no

---

[78] A diferencia de lo que sucede en el ámbito español, donde esta interpretación atentaría contra el bien jurídico, en la noción de datos de la § 202a (2) StGb son susceptibles según la doctrina de ser englobados no solo los datos personales o secretos sino también aquellos que son de libre acceso, por ejemplo, en Internet. Además, tales datos no tienen por qué ir necesariamente referidos a datos individuales sobre las relaciones personales y objetivas, sino que pueden ser de cualquier clase: compilaciones, de conocimiento científico, documentación o resultados de cálculo. También incluye datos que no tienen ningún valor económico o científico o sentimental. ALTENHAIN y WIETZ, 2013: o párrafo 2.. BOSCH, 2014: 1275 o párrafo 2.. FISCHER, 2015: página 1395 o párrafo 2.. GRAF, 2012: 180-181 o párrafo 10.. HEGER, 2014: 965 o párrafo 2.. HILGENDORF, 2005: 1442 o párrafo 8..

[79] Tanto música, vídeo o películas, como otro tipo de datos digitales. KARGL, 2013b: 1407 o párrafo 4..

[80] GRAF, 2012: 180-181 o párrafo 10..

[81] HOYER, 2012: 3 o párrafo 3 (Abschnitt 15).. GRAF, 2012: 180-181 o párrafo 10.. KARGL, 2013b: 1407 o párrafo 4.. WEIDEMANN, 2010: 1306 o párrafo 3..

[82] ALTENHAIN y WIETZ, 2013: o párrafo 2.. FISCHER, 2015: página 1396 o párrafo 4.. HEGER, 2014: 965 o párrafo 2.. HILGENDORF, 2005: 1442 o párrafo 10..

directamente perceptible o bien porque se encuentran siendo transmitidos de una forma no directamente perceptible[83]. Desglosando en partes dicha limitación, puede decirse que ello significa:

b.1) Almacenamiento: es el registro, incorporación o grabado de los datos en un soporte o dispositivo digital o analógico de cualquier tipo[84] con el propósito de su conservación, procesamiento y/o uso posterior[85].

b.2) Transmisión: debe entenderse como tal la transferencia a través de la conexión a una red de área local o de telecomunicaciones por vía electrónica o no corporal de datos almacenados u objeto de procesamiento hacia una localización diferente a los efectos de ponerlos a disposición del examen de o acceso a los mismos por parte de un tercero[86].

b.3) Ausencia de percepción directa: significa que sólo se protegen aquellos datos cuyo acceso a la percepción sensorial puede producirse únicamente mediante la utilización de dispositivos técnicos que permitan la transformación o ampliación de los mismos por parte de

---

[83] BOSCH, 2014: 1275 o párrafo 2.. HILGENDORF, 2005: 1442 o párrafo 10..

[84] Así como la naturaleza y formato del soporte es irrelevante se afirma que la idoneidad como objeto del delito se mantendrá únicamente cuando el almacenamiento continúe. ALTENHAIN y WIETZ, 2013: o párrafo 2.. FISCHER, 2015: página 1396 o párrafo 5.. HILGENDORF, 2005: 67 o párrafo 13.. WEIDEMANN, 2010: 1307 o párrafo 5..

[85] BOSCH, 2014: 1276 o párrafo 3.. FISCHER, 2015: página 1396 o párrafo 5.. GRAF, 2012: 183 o párrafo 18.. HOYER, 2012: 3 o párrafo 4 (Abschnitt 15).. KARGL, 2013b: 1407 o párrafo 6..

[86] Quedan excluidos de la definición los datos que todavía no se han introducido (input data) y los datos que ya han sido enviados (output data). ALTENHAIN y WIETZ, 2013: o párrafo 2.. BOSCH, 2014: 1276 o párrafo 3.. FISCHER, 2015: página 1396 o párrafo 6.. GRAF, 2012: 183 o párrafo 18.. KARGL, 2013b: 1407 o párrafo 6.. HOYER, 2012: 3 o párrafo 4 (Abschnitt 15). SCHÖNKE y SCHRÖDER, 2010: 1819.. WEIDEMANN, 2010: 1307 o párrafo 4.

una persona media[87]. Ello implica, asimismo, la existencia de algún tipo de transformación técnica de los datos por cualquier medio, aunque el tipo no distingue qué tipo de tecnología debe haberse utilizado para ello[88].

C) VALORACIÓN PERSONAL

A mi juicio, estas definiciones resultaban excesivamente amplias para ser trasladada al derogado apartado 3 del artículo 197, pues el bien jurídico del delito era la intimidad. Personalmente, las razones por las que la definición contenida en la § 202a (2) no me parecía extrapolable al ámbito español eran las siguientes:

1. No permitía identificar correctamente qué debe entenderse por dato: tal y como ha puesto de relieve la doctrina alemana, se trata de una conceptualización marcada por la indeterminación y la ausencia de demarcación del propio objeto definido: por un lado, no se especifica ninguna característica de corte positivo que permita delimitar el alcance y contenido del concepto de dato; por otro lado, las limitaciones a las que este se somete no permiten establecer vinculación alguna entre dato informático y acceso ilícito.

2. Es incompatible con la noción de dato del artículo 197.3 del Código penal español: el legislador alemán ha otorgado un contenido muy amplio al concepto de dato informático, que implica entender englobados no solo personales sino de cualquier tipo, incluso los datos públicos. Esta interpretación resulta incompatible con el tipo español de acceso ilícito a un sistema informático del artículo 197.3, por cuanto su ubicación, como se ha reseñado tantas veces, es el Título relativo a la intimidad.

---

[87] GRAF, 2012: 181 o párrafo 13.. HILGENDORF, 2005: 1442 o párrafo 11.. HOYER, 2012: 3 o párrafo 4 (Abschnitt 15).. KARGL, 2013b: 1407 o párrafo 5.. KINDHÄUSER, 2013: 764.. SCHÖNKE y SCHRÖDER, 2010: 1819.. WEIDEMANN, 2010: 1307 o párrafo 4..

[88] FISCHER, 2015: página 1396 o párrafo 4.. GRAF, 2012: 181 o párrafo 12..

3. No se adapta a la definición propuesta por el Convenio de Budapest sobre Cibercriminalidad de 23 de noviembre de 2001, ni la Directiva 2013/40/UE del Parlamento Europeo y del Consejo, de 12 de agosto de 2013, relativa a los ataques contra sistemas de información: la § 202a (2) del Código penal alemán restringe en demasía la noción de dato informático prevista en la normativa supranacional debido a que: a) Mientras en el ámbito alemán su definición se focaliza únicamente en la información, la noción supranacional de dato es más abierta, entendiendo englobada cualquier representación (hechos, informaciones o conceptos) susceptible de procesamiento automatizado. b) Ninguna de las dos normas enunciadas hace referencia a las abstractas restricciones a las que el Código penal alemán ha sometido dicho concepto, especialmente la ausencia de perceptibilidad, lo que conduce a dejar fuera del ámbito típico todo un conjunto de datos que también deberían ser considerados informáticos. Desde esta perspectiva, la restricción del concepto de dato no parece adecuada.

4. Parece, pues, que el legislador alemán, aún habiendo ido un paso más allá que el español al pretender positivizar el concepto de datos informáticos, en realidad ha cometido los mismos errores que éste a la hora de configurar el concepto de datos informáticos, que adolece de las mismas deficiencias que el artículo 197.3: excesiva generalidad y delimitación mediante una interpretación de carácter negativo.Así pues, tanto el Convenio sobre Cibercrimen de Budapest, de 23 de noviembre de 2001, y la Directiva, 2013/40/UE, de 12 de agosto de 2013, del Parlamento Europeo y del Consejo, relativa a los ataques contra los sistemas de información y por la que se sustituye la Decisión marco 2005/222/JAI del Consejo.

Por lo que se refiere a la definición supranacional, la noción de dato parecía más ajustada a las pretensiones de incriminación del legislador español. Teniendo en cuenta la extrema amplitud de la misma, creo que ésta definición sería válida para poder definir el concepto de dato informático contenido en un sistema informático, siempre que no se olvidase la mención de los elementos de interpretación a los que se ha hecho referencia y que son:

> **1. Bien jurídico:** puesto que el artículo 197.3 tenía como objeto de protección la intimidad o, más bien la privacidad, la definición de dato debía vincularse a ésta[89].
>
> **2. Elemento negativo de la definición:** no podía olvidarse en la definición de dato la puesta en relación de este apartado con los apartados 1 y 2 del artículo 197 pues el apartado 3 conformaba un tipo residual de los restantes apartados del precepto cuyo ámbito típico debía fijarse en atención a una delimitación sistemática negativa[90].

En consecuencia, los datos informáticos *ex* artículo 197.3 del Código penal serían aquel **conjunto de informaciones, hechos o representaciones de la privacidad susceptibles de tratamiento automatizado a través de la utilización de un sistema informático, excluidos los datos informáticos protegidos en los apartados 1 y 2 del artículo 197**.

---

[89] Véase Capítulo III. Sección 1ª.

[90] Véase Apartados precedentes de este Capítulo.

SECCIÓN 2ª

EL OBJETO MATERIAL DEL DELITO DE ACCESO ILÍCITO EN LA REFORMA OPERADA POR LA LEY ORGÁNICA 1/2015, DE 30 DE MARZO

I. INTRODUCCIÓN

He puesto de relieve con anterioridad, que el delito de acceso ilícito informático no es un hecho contrario a la intimidad de las personas. Una de las razones que sustenta esta tesis es la configuración del objeto material, pues no se trata de un delito que castiga el acceso a datos informáticos, sino el acceso al propio sistema informático.

Es por ello que, en coherencia con lo que yo misma he propuesto de relieve en estudios anteriores[1], la reforma operada por la Ley Orgánica 1/2015, ha modificado acertadamente el objeto material del delito para adecuarlo a las exigencias de la normativa supranacional, sancionando así el acceso al propio sistema informático y no a los datos contenidos en éste. Este hecho ha permitido solventar los extremadamente complejos problemas interpretativos señalados en el apartado anterior.

No obstante, en la actual redacción vigente del artículo 197.1 bis no se hace referencia directa al sistema informático, sino al sistema de información. Ello es consecuencia del acogimiento de la terminología usada por la Directiva, 2013/40/UE, de 12 de agosto de 2013, del Parlamento Europeo y del Consejo, relativa a los ataques contra los sistemas de información y por la que se sustituye la Decisión marco 2005/222/JAI del Consejo, herencia de ésta última, en lugar de la del Convenio sobre Cibercrimen de Budapest, de 23 de noviembre de 2001.

Así pues, delimitado en el apartado anterior el objeto material del delito conforme a la redacción típica vigente entre los años 2010 y 2015, resta ahora precisar el concepto y el contenido de este nuevo y mejor adaptado objeto material: el sistema informático. Pero, antes de ello, será necesario analizar el concepto de sistema de información vs. el de sistema informático para descifrar exactamente a qué se están refiriendo cada una de las normas enunciadas.

---

[1] Véase MONTSERRAT SÁNCHEZ-ESCRIBANO, 2014. MONTSERRAT SÁNCHEZ-ESCRIBANO, 2015.

II. CONCEPTO EN LA NORMATIVA SUPRANACIONAL

El punto de partida para ofrecer una visión del objeto material del delito objeto de estudio, el acceso ilícito a un sistema informático, debe ser la normativa supranacional, es decir, el Convenio sobre Cibercrimen de Budapest, de 23 de noviembre de 2001, y la Directiva, 2013/40/UE, de 12 de agosto de 2013, del Parlamento Europeo y del Consejo, relativa a los ataques contra los sistemas de información y por la que se sustituye la Decisión marco 2005/222/JAI del Consejo.

A) SISTEMA DE INFORMACIÓN VS. SISTEMA INFORMÁTICO

El primer dato que se observa si se comparan una y otra norma es la utilización de una diferente nomenclatura para definir el objeto al que va referida la acción: mientras el Convenio adopta como tal el sistema informático[2], la Directiva, en cambio, maneja el concepto de sistema de información[3], designación que, a su vez, constituye herencia directa de la Decisión Marco arriba citada[4].

Esta discrepancia en la denominación hace nacer de inicio una serie de vicisitudes, que se desprenden de la posibilidad de que ambos conceptos puedan considerarse sinónimos o, por el contrario, deban interpretarse como términos divergentes. En el primer caso, el

---

[2] *Article 2 – Illegal access*

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the access to the whole or any part of a ***computer system*** *without right.*

[3] *Artículo 3 Acceso ilegal a los* ***sistemas de información***

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.*

[4] *Artículo 2 Acceso ilegal a los* ***sistemas de información***

1. Cada Estado 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.*

alcance de la tutela penal deberá plantearse de forma uniforme, pero si se concluye que se trata de nociones con un significado distinto habrá que buscar un encuadre en la configuración del tipo penal que satisfaga las pretensiones tanto del Convenio como de la Directiva, hecho que podría complicar bastante la determinación de la esfera aplicativa del delito.

Pues bien, para poder arbitrar una respuesta a esta pregunta es necesario acudir a los respectivos artículos 1 y 2 de las susodichas normas, los cuales recogen las definiciones de los distintos elementos materiales que integran las propuestas de incriminación que realiza a lo lardo de su articulado[5]. Analizándolas conjuntamente un hecho divergente entre una y otra es en que la Directiva incluye como un elemento más, además de los diversos componentes físicos de los que se integra el sistema informático y que se conocen como *hardware*, a los datos informáticos almacenados, tratados, recuperados o transmitidos por dicho aparato o grupo de aparatos para su funcionamiento, utilización, protección y mantenimiento.

Esta delimitación tan precisa de los datos informáticos que forman parte integrante del sistema suscita la duda de si los datos a los que hace referencia son datos de *software* con la única función es viabilizar la operatividad del sistema informático o datos de contenido, que el usuario del mismo ha creado. Para resolver este enigma resulta imprescindible profundizar en la definición de sistema de información ofrecida por la Directiva.

---

[5]Artículo 1 a) del Convenio sobre Cibercrimen:*"computer system" means any device or a group of interconnected or related devices, one or more of which, pursuant to a program, performs automatic processing of data.*

Artículo 2 a) de la Directiva 2013/40/UE*: «sistema de información»: todo aparato o grupo de aparatos interconectados o relacionados entre sí, uno o varios de los cuales realizan, mediante un programa, el tratamiento automático de datos informáticos, así como los datos informáticos almacenados, tratados, recuperados o transmitidos por dicho aparato o grupo de aparatos para su funcionamiento, utilización, protección y mantenimiento.*

1. CONCEPTO DE SISTEMA DE INFORMACIÓN

a) CONCEPTO LEGAL DE SISTEMA DE INFORMACIÓN

La Directiva 2013/40/UE, de 12 de agosto de 2013, podría haber limitado la alusión a los datos informáticos en la definición del concepto de sistema de información a una referencia genérica, pues la definición de datos informáticos aparece recogida a continuación de ésta[6]. Sin embargo, el hecho de que precise cuáles son los datos que deben quedar incluidos en la configuración de la noción de sistema es un dato muy indicativo.

Como se observa, la Directiva utiliza dos parámetros para definir sistema de información:

> a) Por una parte, el conjunto de 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.
>
> b) Por otra, los datos informáticos que tienen como finalidad asegurar su funcionamiento, utilización, protección y mantenimiento.

---

[6] En ella se define genéricamente dato informático 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*.

i) CONCEPTO Y TIPOLOGÍA DE SOFTWARE INFORMÁTICO

El **software** es la parte inmaterial o lógica del sistema informático y suele definirse como aquel conjunto de datos y programas que son necesarios para que la parte física del sistema informático realice su función[7]. El software está estructurado de forma jerárquica pudiéndose distinguir, básicamente, dos tipos de software[8]:

a) El **software base:** proporciona los servicios básicos de todos los sistemas informáticos y que incluye el sistema operativo, el compilador, el gestor de arranque del sistema y los montadores[9].

b) El **software de aplicación** es el resultado del software de desarrollo, el cual mediante el uso del lenguaje de programación, originan las aplicaciones que usan los usuarios del sistema informático, permitiéndoles obtener la utilidad del sistema[10].

---

[7] DE PABLOS HEREDEROS, 2004: 100.

[8] A ellos en ocasiones puede añadirse el denominado software de desarrollo, también llamado lenguaje de programación o sistema de desarrollo, pues es el software que se utiliza para desarrollar los programas o software de aplicación. AMAYA AMAYA, 2010: 31.

[9] El más importante de ellos es el **sistema operativo** que es el programa supervisor que asegura el funcionamiento del sistema informático mediante la repartición y asignación de los recursos de hardware del sistema y el monitoreo de las actividades de éste. El sistema operativo tiene básicamente las siguientes funciones: soportar operaciones básicas de entrada y salida, repartir/asignar el almacenamiento y la memoria, y posibilitar a las distintas aplicaciones el uso compartido del ordenador.

El **compilador** es el programa que traduce un programa escrito en lenguaje de alto nivel a las instrucciones básicas que el hardware puede ejecutar.

El **gestor de arranque** es un programa que traduce una versión simbólica de instrucciones al código binario.

DE PABLOS HEREDEROS, 2004: 101-102. PATTERSON y HENNSSY, 2014: 13-14.

[10] PATTERSON y HENNSSY, 2014: 13-14.

ii) APLICACIÓN A LA DEFINICIÓN DE SOFTWARE

En mi opinión, la definición de sistema informático que ofrece la Directiva se está refiriendo al propio software y no a los datos de contenido. En realidad, el software no está integrado más que por un conjunto de datos que interconectados entre sí crean las secuencias de instrucciones en las que consisten los lenguajes de programación que constituyen el soporte para el software[11].

Pero la misión que todos estos datos tienen se concentra en las cuatro características que la determinación de los datos a los que se refiere la definición de sistema de información *in fine*: funcionamiento, utilización, protección y mantenimiento del sistema[12]. Lograr el funcionamiento y mantenimiento del sistema es, concretamente, la misión que tiene atribuida el software base, mientras que proporcionar protección y utilización del sistema podría considerarse una función compartida entre el software base y el software de aplicación.

En consecuencia, con independencia de cual fuera su intención, a mi parecer la Directiva no está haciendo más que ahondar en el propio concepto software y no refiriéndose al contenido del sistema creado por el usuario, producto de los programas o software de aplicación, que serán objeto de estudio en el apartado III de este capítulo[13].

---

[11] El sistema operativo funciona con lo que se denomina comandos. Los comandos son datos que a modo de órdenes se introducen en el sistema y que permiten al usuario realizar operaciones en el mismo, en el cual el programa intérprete de comandos contiene un código para ejecutar el comando.

[12] GARRIDO CARRILLO, 2006: 3.

[13] Véase Apartado III de este Capítulo.

b) CONCEPTO TÉCNICO DE SISTEMA DE INFORMACIÓN

El concepto de sistema de información, al igual que el de sistema informático, tiene como raíz el concepto de sistema[14], el cual puede definirse como un conjunto de elementos que interaccionan entre sí para lograr un objetivo común con base a dos aspectos: uno estructural, esto es, la manera en que estos distintos componentes del sistema se interrelacionan, y otro funcional, la función que cada uno tiene de forma individual en la estructura[15]. Conforme a la definición ofrecida pueden encontrarse en la sociedad actual multitud de sistemas, de entre los cuales el que aquí interesa es el sistema de información.

---

[14] La formulación del concepto de sistema fue llevada a cabo ya en la década de los 40 por Von Bertalanffy, creador de la conocida teoría general de los sistemas. Aunque el concepto de sistema tiene una larga tradición en la historia de la filosofía, especialmente en el ámbito de la filosofía natural (donde este concepto incluye muchos nombre ilustres), y aun a pesar de que se puede encontrar alguna que otra obra preliminar en el terreno de la teoría de los sistemas, no es sino hasta la formulación de la susodicha teoría por parte de von Bertalanffy que se puede hablar de un estudio interdisciplinar que parte del concepto abstracto de sistema para hallar las propiedades comunes a estas entidades. La teoría general de los sistemas de Von Bertalanffy no solo ha sentado las bases de la propia noción de sistema, sino que, además, ha sido la base para el desarrollo de los posteriores ámbitos tecnológicos de las ciencias, como la ingeniería de sistemas y todos los campos afines a ésta. En este sentido, como se verá, la aportación de Von Bertalanffy tiene también su reflejo en las definiciones de sistema informático y de sistema de información contenidas en la normativa supranacional. Por este motivo, el desarrollo de este trabajo no puede obviar las importantes consecuencias que esta definición ha tenido también en el ámbito del Derecho. VON BERTALANFFY, 1945:. VON BERTALANFFY, 1950:. VON BERTALANFFY, 1951:. VON BERTALANFFY, 1968:. VON BERTALANFFY, 1975:.

15 Como puede deducirse, existe una gran variedad de sistemas, la mayor parte de los cuales pueden desmembrarse en atención a las dos características mencionadas en los siguientes elementos: elementos de entrada, a través de los cuales entran los recursos; sección de transformación, que modifica tales recursos; mecanismo de control, que supervisa el proceso de transformación para que se lleve a cabo conforme al objetivo; y elementos de salida, por donde sale el resultado del proceso de dicho proceso. FERNÁNDEZ ALARCÓN, 2006: 11.

Aunque no existe consenso unánime sobre su definición, y, además, puede ser definido desde multitud de perspectivas[16], se puede decir que el sistema de información no integra más que un subgénero o una subespecie de sistema cuya característica principal es la de satisfacer la necesidad de información de una organización[17]. En este sentido, aunque hoy en día este concepto se aplique cada vez a más campos[18], el ámbito natural y en el que le ha propiciado mayor desarrollo es el empresarial[19], integrando uno de los distintos subsistemas en los que ésta se divide[20].

---

[16] La primera definición de sistema de información nace en el seno de las Ciencias de la Información y la Documentación. Concretamente, se cita como precursor el concepto creado por BORKO sobre esta última: *disciplina que investiga las propiedades y el comportamiento de la información, las fuerzas que gobiernan el flujo de la misma y los medios que la procesan para lograr la mayor optimización en su accesibilidad y uso*, y que tiene por objeto l*a creación, recolección, organización, almacenamiento, recuperación, interpretación, transmisión, transformación y utilización de dicha información*. Desde entonces, han sido numerosas y variadas las nociones ofrecidas en la literatura científica, si bien, de entre todas ellas, la que más se repite es la de CODINA BONILLA: *conjunto de elementos y procesos que intervienen dinámicamente en la explotación de información cognitiva concebida en el marco de un grupo social concreto y para áreas determinadas, cuyo propósito es facilitarles el acceso al conocimiento y apoyarlos en la toma correcta de decisiones*. BORKO, 1965: 3, 5. CODINA BONILLA, 1996: 124. Sobre la definición, veáse: FERNÁNDEZ ALARCÓN, 2006:. HERNÁNDEZ TRASOBARES, 2003:. LÓPEZ YÉPEZ, 1991:. TRAMULLAS SAZ, 1997:.

[17] Sobre este particular MORALES LÓPEZ, 2010: 143-169.

18 Ya BORKO citaba como ejemplos las matemáticas, la lógica, la lingüística, la psicología, la computación tecnológica, las operaciones de investigación, las artes gráficas, las comunicaciones, la biblioteconomía y la administración y dirección de empresas. BORKO, 1965: 3.

[19]De entre todas, la definición más conocida y precisa en el ámbito económico es la de ANDREU, RICART y VALOR *como el conjunto formal de procesos que, operando con un conjunto estructurado de datos estructurado de acuerdo con las necesidades de una empresa, recopila, elabora y distribuye (parte de) la información necesaria para la operación de dicha empresa y para las actividades de dirección de control correspondientes, apoyando al menos en parte, la toma de decisiones necesaria para desempeñar las funciones y procesos de negocio de la empresa de acuerdo con su estrategia*. ANDREU et al., 1996: 13.

[20] LAPIEDRA ALCAMÍ et al., 2011: 13.

En el seno de la organización empresarial, el sistema de información tiene como función tratar una gran cantidad de datos y proporcionar información con diferentes estructuras a los múltiples órganos de los que se compone la empresa, ya sea para ser usada en la toma de decisiones a nivel operativo, directivo y estratégico[21]. Ahora bien, este resultado final en el que consiste la información, dependerá del concreto entorno de cada organización y se adaptará a las especiales necesidades de cada órgano integrante[22].

Para lograr esta misión el papel de la informática se ha convertido en un instrumento fundamental, pero no imprescindible[23]. El sistema informático es, por tanto, el conjunto de elementos que hacen posible el sistema de información[24], pero la noción de sistema de información está dotada de una mayor extensión, cimentada en la propia idea de organización[25].

---

[21] LAPIEDRA ALCAMÍ et al., 2011: 13. FERNÁNDEZ ALARCÓN, 2006: 14.

[22] LAPIEDRA ALCAMÍ et al., 2011: 13.

[23] En este sentido se suele apuntar que el sistema de información es anterior al del sistema informático en tanto en cuanto éste ha existido desde mucho antes de la computación. A tal efecto, entre las distintas tipologías que sirven de clasificación a los sistemas de información, se distingue entre sistemas manuales e informatizados, aunque a día de hoy sea muy inferior (por no decir prácticamente nulo) el número de sistemas de información no informatizados que puedan encontrarse. La tecnología informática, se afirma, ha potenciado de una forma tan extraordinaria la capacidad y exactitud del tratamiento de los datos, que resulta inconcebible el diseño de un sistema de información sin la utilización de la misma. ROS GARCÍA, 1996: 37.

[24] El sistema informático, como se verá en las próximas páginas, solo conforma uno de los distintos elementos de los que el sistema de información está constituido. La delimitación de los distintos componentes del sistema de información se realiza conforme a los postulados de Whitten, Bentley y Dittman: personas, datos, procesos y tecnologías de la información. FERNÁNDEZ ALARCÓN, 2006: 15-21.

[25] TRAMULLAS SAZ, 1997: 218.

2. RELACIÓN DE LOS CONCEPTOS DE SISTEMA DE INFORMACIÓN Y SISTEMA INFORMÁTICO

Conforme a esta explicación, aunque ambos conceptos tienen una raíz común, la noción de sistema, es posible diferenciar conceptualmente el sistema de información del sistema informático y concluir que no resultan términos equiparables[26]. A esta conclusión ha llegado unánimemente la doctrina científico-económica que se ocupa del análisis de cuál es el rol del sistema de información en la organización, habiéndose publicado por parte de MONTERO CARRIÓN incluso un artículo específico a este respecto[27]. Aunando las ideas de este autor con algunas de las ya expuestas y otras que las complementan, pueden señalarse como principales diferencias entre ambos términos las siguientes:

> **a) Necesidad:** el sistema de información puede cumplir su función sin necesidad de realizar el tratamiento de los datos a través de un sistema informático, si bien su eficiencia se verá reducida notablemente[28].
>
> **b) Instrumentalidad:** el sistema informático es meramente el medio a través del cual cumple su función el sistema de información, pudiendo éste cumplir esta misma misión a través de otros medios o instrumentos[29].

---

26 De hecho, esta circunstancia es algo que pone de relieve unánimemente toda la literatura económica: LAPIEDRA ALCAMÍ et al., 2011: 14-15.

27 MONTERO CARRIÓN, 2008:.

28 LAPIEDRA ALCAMÍ et al., 2011: 15.

29 ROS GARCÍA, 1996: 37.

c) Alcance: el sistema de información de la empresa es el conjunto de recursos y procedimientos utilizados en el tratamiento de información[30] e integra recursos humanos, económicos, tecnológicos, funciones y semánticos dirigidos a tal fin[31], esto es, la organización[32]. El sistema informático está integrado únicamente por los aspectos procedimentales del conjunto mencionado, esto es, por un conjunto de elementos físicos (hardware) que, interconectados entre sí, interactúan mediante el uso de elementos lógicos (software) para realizar el tratamiento de información[33].

d) Resultados: mientras que el sistema informático es un sistema determinista en el que un *input* determinado siempre se obtiene un mismo *output*, el sistema de información está influido en gran medida por los objetivos, valores y creencias de los distintos individuos y órganos que integran la organización[34], de modo que el el resultado del tratamiento de la información dependerá de las necesidades de cada órgano concreto[35], existiendo, además, un proceso de retroalimentación o *feedback*, en la cual se ha de valorar si la información obtenida se adecua a lo esperado[36].

---

[30] MONTERO CARRIÓN, 2008: 78.

[31] ROS GARCÍA, 1996: 39.

[32] TRAMULLAS SAZ, 1997: 218.

[33] Ver próximo apartado.

[34] LAPIEDRA ALCAMÍ et al., 2011: 14.

[35] LAPIEDRA ALCAMÍ et al., 2011: 15.

[36] HERNÁNDEZ TRASOBARES, 2003: 1.

3. CONCLUSIÓN

Conforme a todo lo apuntado hasta el momento, debe concluirse que la denominación utilizada por la Directiva 2013/40/UE, de 12 de agosto, refiriéndose a sistema de información y no a sistema informático es de todo punto incorrecta, pues, recogiendo en la definición los elementos básicos de los que se integra el sistema informático, está haciendo alusión a una realidad más amplia que éste.

El concepto de sistema de información, específicamente creado sobre la base de la teoría de la organización, tiene su base en ésta y no puede independizarse de ella. Su función es el tratamiento de información para satisfacer las distintas necesidades de los recursos humanos de los que ésta dispone. No puede eliminarse, por tanto, la estructura del sistema de información así como el componente humano que lo caracteriza por uno de los instrumentos a través de los cuales éste cumple su función: el sistema informático. Y tampoco puede obviarse que el resultado proporcionado por el sistema de información será distinto como respuesta a la adaptación de la concreta petición de cada órgano en concreto.

A lo anterior se une, finalmente, que no debe inducir a error el hecho de que hoy en día la mayor parte de los sistemas de información estén informatizados por razones de eficiencia con el hecho de que ambos conceptos se consideren equivalentes. El sistema informático puede formar parte del sistema de información o no, siendo que su integración en la estructura organizativa sea conveniente a efectos de cumplir con mayor corrección y celeridad su función.

En consecuencia, el concepto asumido por el artículo 197.1 bis es también erróneo, de tal forma que éste hubiera debido utilizar el de sistema informático. En cualquier caso, el concepto de sistema de información resulta incompatible con la pretensión de tutela pretendida por éste, motivo por el cual deberá ser interpretado restrictivamente conforme al contenido atribuido a aquel.

B) CONCEPTO DE SISTEMA INFORMÁTICO

Precisada cual es la terminología correcta a emplear y despejada toda duda en cuanto a las posibles incongruencias que la Directiva 2013/40/UE, de 12 de agosto, podría introducir en la fijación del objeto material del delito, el siguiente paso supone detenerse en la concreta definición de sistema informático. Sin olvidar la definición del Convenio: *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*.

En mi opinión, el punto de partida más adecuado es la noción utilizada en la Ciencia de donde éste tiene su origen, la Ingeniería Informática de Sistemas[37], que lo define como un conjunto de dispositivos informáticos de carácter físico (hardware) y lógico (software) relacionados entre sí que tienen como función el procesamiento, almacenamiento, el movimiento, la transmisión y el control de los datos[38].

Al igual que en la noción de sistema de información, es posible diferenciar los dos aspectos de todo sistema: el estructural y el funcional[39], que se pasan a comentar.

---

[37] En el ámbito de la informática a estudiar esta jerarquía y las cuestiones relacionadas con la partición de de los distintos niveles dentro de un sistema informático y cómo es implementado cada elemento dentro de éstos es a lo que se dedica la ciencia denominada organización de computadoras (*computer organization*). En cambio, el segundo nivel, el funcional, es estudiado por la ciencia denominada arquitectura de la computación (*computer architecture*), que centra su estudio en la interacción entre hardware y software, enfatizando específicamente en a estructura y el comportamiento del sistema informático. NULL y LOBUR, 2015: xvii.

[38] STALLINGS, 2013: 8-9.

[39] Uniendo ambas definiciones, el elemento estructural vendría a integrarse por el conjunto de elementos que aparatos interconectados o relacionados entre sí mediante un programa, mientras que el elemento funcional, relativo al tratamiento automatizado de datos vendría a expresarse en el procesamiento, almacenamiento, el movimiento, la transmisión y el control de los datos.

1. ASPECTO ESTRUCTURAL: COMPONENTES DEL SISTEMA

El sistema informático está integrado por cuatro elementos[40]:

a) Software o elementos lógicos: los programas y datos que se contienen en el hardware.

b) Hardware o elementos físicos: dispositivos electrónicos y mecánicos que realizan los cálculos y el manejo de la información.

c) Elemento personal: usuarios que interactúan con los equipos hardware, y expertos informáticos que desarrollan y mantienen el software (para que esa interacción sea posible).

d) Información descriptiva: conjunto de manuales técnicos o de usuario, formularios, documentación de procedimientos o cualquier soporte que dé instrucciones sobre el uso del sistema informático.

Los distintos elementos que integran el sistema informático **interaccionan** entre ellos por medio de lo que se denomina **lenguaje de programación**, que puede dividirse entre lenguaje de alto nivel (el que utiliza el software) o lenguaje básico o del hardware, un conjunto de señales eléctricas y que utiliza únicamente 0 y 1, conocido como código binario o bit[41]. La combinación de estos números hace comportarse al sistema de una u otra manera, llamándose las distintas combinaciones comandos y que cuando se unen crean lo que se denomina instrucciones, que son solo colecciones de bits que el sistema entiende y obedece[42].

---

[40] STALLINGS, 2013: XIII.

[41] PATTERSON y HENNSSY, 2014: 14.

[42] PATTERSON y HENNSSY, 2014: 14.

2. ASPECTO FUNCIONAL: FUNCIONES DEL SISTEMA

Pero para que un conjunto de elementos interconectados entre sí pueda ser considerado como un sistema informático es necesario no sólo que esté dotado de los elementos anteriores, sino que tales elementos interaccionen entre sí a los efectos de conseguir el tratamiento automatizado de datos. Por consiguiente, desde un punto de vista funcional, la interpelación entre el software y el hardware que interaccionan entre sí mediante el lenguaje de programación tienen que tener como finalidad permitir el **tratamiento automatizado de datos** a través de la realización de las siguientes funciones: procesamiento de datos, almacenamiento de datos, movimiento o transmisión de datos y control de las funciones anteriores[43].

---

[43] Las funciones que tiene encomendadas el sistema son las siguientes:

a) Procesamiento de datos: los datos toman una variedad de forman y el rango de procesamiento que el sistema informático usa es amplio.

b) Almacenamiento de datos: es uno de las funciones más esenciales del sistema informático, y puede dividirse en dos categorías: almacenamiento a corto plazo, caso en el que temporalmente el sistema almacena piezas de datos sobre la marcha relativos a piezas de datos sobre las que se está trabajando en un momento dado y almacenamiento a largo plazo, caso en el que los archivos de datos se almacenan en el ordenador para su recuperación y actualización posterior.

c) Movimiento o transmisión de datos: todo sistema informático tiene que ser capaz de transmitir datos entre sí mismo y el resto del mundo. y, en consecuencia, debe constar de dispositivos que le permiten ser fuente o destino de datos, ya sea a través de un proceso de entrada y salida (input–output (I/O) process) por un dispositivo que está conectado directamente al ordenador (dispositivo periférico) o a través de un dispositivo remoto (comunicación de datos).

d) Control: todas las funciones anteriores deben ser controladas, misión que tiene encomendada la unidad de control, la cual es ejercida ejercido por el individuo que proporciona al sistema las instrucciones y, más concretamente, por la unidad de control, gestiona los recursos del ordenador y orquesta el cumplimiento de sus partes funcionales en respuesta a dichas instrucciones.

STALLINGS, 2013: 11.

3. CONCRECIÓN DEL CONCEPTO DE SISTEMA INFORMÁTICO

El sistema informático se presenta así como un conjunto de capas y elementos jerárquicamente organizados sobre la base de una estratificación virtual, que empieza en el nivel más bajo en que consiste el hardware y que termina en un nivel alto de procesamiento de datos a través del software[44]. Estos son los dos componentes que deben integrar todo sistema informático y de los cuales éste no puede prescindir[45]. Desde esta perspectiva, sistema informático no debe entenderse como sinónimo de ordenador personal, sino que cualquier tipo de dispositivo que cumpla las características mencionadas queda amparado en la definición ofrecida[46].

---

[44] NULL y LOBUR, 2015: xvii.

[45] A los efectos de explicar la interrelación existente entre ambos elementos, en informática se habla del principio de equivalencia del software y el hardware, según el cual cualquier tarea llevada a cabo por el software puede ser también realizada usando hardware, y cualquier operación realizada directamente por el hardware puede ser hecha usando software. NULL y LOBUR, 2015: 3.

[46] Los sistemas informáticos pueden sistematizarse desde la perspectiva de la arquitectura de la computación (del hardware) en atención a tres tipos:

> **a) Ordenadores y dispositivos personales (PC):** ordenadores diseñados para el uso individual, normalmente incorporando un diseño gráfico, un teclado y, en ocasiones, un ratón. Son el ordenador, el móvil, la tablet.
>
> **b) Servidores:** sistemas con acceso únicamente usando una red de área local o global y que tienen como única función soportar inmensos volúmenes de trabajo consistentes en facilitar el uso de aplicaciones complejas únicas o el trabajo individual de muchos pequeños trabajos basados normalmente en software procedente de otra fuente. Su principal misión es el almacenamiento y la capacidad input/output. Como ejemplos pueden citarse Amazon, google.
>
> **c) Sistemas informáticos incrustados:** consisten en sistemas informáticos que forman parte de otro dispositivo o sistema y que son usados para ejecutar una determinada aplicación o colección de software. Son diseñados para ejecutar una aplicación o un conjunto de aplicaciones que normalmente con el hardware y entregadas como un sistema único. Suponen por ejemplo, los microprocesadores de los coches, los incluidos en la TV, en las redes de control de los aviones o en un barco.

PATTERSON y HENNSSY, 2014: 5.

III. SISTEMA INFORMÁTICO: OBJETO MATERIAL DEL DELITO

Como se ha indicado, el objeto material del delito de acceso ilícito es el sistema informático y como tal puede ser considerado cualquier dispositivo que esté dotado de dos elementos: software y hardware. El siguiente paso lo constituirá, por tanto, delimitar qué debe entenderse como software y hardware a efectos de establecer qué es jurídico-penalmente un sistema informático en tanto objeto material del delito de acceso ilícito a un sistema informático.

En consecuencia, será necesario ofrecer una noción jurídico-penal de software y de hardware, que paso a comentar, definición en la que no quedarán englobados todos los elementos a los que se ha hecho referencia en la definición de sistema informático, pues no todos ellos pueden ser trasladados el ámbito jurídico penal. Me refiero, concretamente, al factor personal y a los manuales de usuario.

La noción penal de sistema informático debe centrarse, por tanto, únicamente en el software y en el hardware del sistema. La creación de un concepto sobre la base de estos dos aspectos ha tenido un profundo acogimiento en la doctrina y jurisprudencia de otros

países, entre los que cabe destacar Italia[47] o Francia[48]. En cualquier caso, por sistema informático no debe confundirse con ordenador

[47] En general, ésta suele ser la definición ofrecida por la doctrina (CARINGELLA). CARINGELLA et al., 2011: 1052. Sin embargo, la definición que en el ámbito italiano más se repite es la de la Cass. Sez. VI 14 diciembre 1999, nº 3067, in Cass. Pen., 2000, 2990: *un complesso di apparecchiature destinate a compiere una qualsiasi funzione utile all'uomo, attraverso l'utilizzazione (anche parziale) di tecnologie informatiche, che sono caratterizzate - per mezzo di un'attività di «codificazione» e «decodificazione» - dalla «registrazione » o «memorizzazione», per mezzo di impulsi elettronici, su supporti adeguati, di «dati», cioè di rappresentazioni elementari di un fatto, effettuata attraverso simboli (bit), in combinazione diverse, e dalla elaborazione automatica di tali dati, in modo da generare «informazioni», costituite da un insieme più o meno vasto di dati organizzati secondo una logica che consenta loro di esprimere un particolare significato per l'utente. La valutazione circa il funzionamento di apparecchiature a mezzo di tali tecnologie costituisce giudizio di fatto insindacabile in Cassazione ove sorretto da motivazione adeguata e immune da errori logici.*

[48] El Código penal francés no hace referencia a sistema informático sino a sistema de tratamiento automatizado de datos. En este país durante el debate parlamentario, en el Senado se propuso como definición la siguiente: *tout ensemble composé d'une ou plusieurs unités de traitement, de mémoire, de logiciel, de données, d'organes d'entrées-sorties et de liaisons, qui concourent à un résultat déterminé, cet ensemble étant protégé par des dispositifs de sécurité*. Tanto la denominación francesa para referirse al sistema informático como la noción ofrecida para su definición son plenamente correctas, puesto que ambas ponen el acento en los componentes y función de éste.

personal[49], sino que cualquier tipo de dispositivo dotado de las características anteriores debe quedar al amparo del anterior[50].

---

[49] La Relazione anotada en la nota anterior hace referencia que el sistema informático se protege con independencia de su contenido, en el sentio de que se protege un sistema informático de cualquier tipo y dimensión, comprendiendo como tal tanto aquellos de uso individual o particular como aquellos que están destinados a fines más complejos destinados a una pluralidad de usuarios como puede ser el de una empresa CANNATA, 2006: 531-532. D'AIETTI, 1994: 69.

[50] El artículo 615 ter del Código penal italiano recoge junto al concepto de sistema informático el de sistema telemático. Éste designa a cualquier forma de telecomunicación que haga uso de la tecnología informática. La doctrina italiana no tiene muy claro a qué ha querido hacer referencia el legislador italiano con esta expresión y se plantean dos tesis al respecto: por una parte, algunos autores entienden que on ello ha pretendido el legislador italiano hacer referencia a los sistemas de transmisión telefónica, móvil y fija, que utilizan la tecnología digital (AMORE, BORRUSO, DESTITO), mientras que otros entienden que se trata de una conexión remota de *teleprocessing* (MANTOVANI y, siguiendo a éste, DI PUNZIO). Incluyen ambos (CECCACCI) No existen en mi opinión inconveniente alguno en poder incluir todos estos aparatos en la definición de sistema informático. La opción por la primera de las dos posiciones expuestas vino a ser confirmada en este país por la *Relazione di presentazione dello Schema di Progetto di legge contenente modificazioni ed integrazioni delle norme del Codice penal in tema di criminalità informatica*, que definió sistema telemático como aquel vinculado a una red de telecomunicación sea pública o privada, local o geográfica, nacional o internacional. AMORE et al., 2006: 98. BORRUSO, 1994: 7-9. CECCACCI, 1994: 71. DESTITO et al., 2007: 83. DI PUNZIO y NATALINI, 2006: 698.

En Francia se han adoptado una concepción extremadamente amplia de sistema informático o partes de éste un disco duro (Cour d'appel de Douai, 7 oct. 1992), un teléfono móvil (Cour d'appel de Paris, 18 nov. 1992) o la banda magnética de una tarjeta bancaria (Trib. cor. Paris, 25 fev. 2000). BEM, 2010: 1.

A) LA PROTECCIÓN JURÍDICO-PENAL DEL SOFTWARE

En el ordenamiento jurídico español la regulación jurídica relativa a la protección del software se ha articulado a través de lo que se conoce como derechos de autor o propiedad intelectual[51]. En este sentido, puesto que el objeto material del artículo 197.1 *bis* resulta en parte coincidente con el de los delitos contra la propiedad intelectual, el recurso al estudio de algunas cuestiones relativas a éstos se hace imprescindible a los efectos de ilustrar el presente trabajo. Tales normas están integradas en gran medida por conceptos normativos de valoración legal[52]: normas compuestas por términos descriptivos con referencias normativas que deben ser completadas en muchos de sus términos recurriendo a la normativa extrapenal en la materia[53]. En este caso, la definición de programa informático en el ámbito de los delitos contra la propiedad intelectual se realiza recurriendo al Derecho civil. Por este motivo, se incorporarán al presente trabajo estas cuestiones de orden civil, ello siempre sin olvidar que el Derecho penal es una ciencia autónoma e independiente de las demás disciplinas jurídicas.

---

51 Se utilizará únicamente la expresión propiedad intelectual en lugar de la de derechos de autor con la finalidad de hacer referencia a la vertiente más amplia de este derecho. Para más información véase

52 Efectivamente, los delitos contra la propiedad intelectual ya no son normas penales en blanco. El artículo 534.1 del Código penal de 1973, precedente del actual artículo 270, sí que será un tipo penal en blanco que incriminaba genéricamente la acción de infringir el derecho penal de autor, sin dotar de contenido alguno a dicho término normativo valorado. La descripción típica debía completarse acudiendo a una dispersa y, a veces, incongruente normativa extrapenal que conducía a subsumir en el tipo cualquier vulneración de tal derecho con independencia de su contenido de injusto. Mediante la reforma de 1987 se abandonó, con algunas excepciones, la técnica de la norma penal en blanco, hecho que se mantuvo posteriormente en el Código penal de 1995. SAN 117/2016, 5 febrero, FJ. 3.2.1.2 Siguen considerando, no obstante, que se trata de una norma penal en blanco:

53 Circular de la Fiscalía General del Estado número 2/1989, de 20 de abril, relativa a las precisiones conceptuales sobre algunos aspectos de la formulación típica y de la responsabilidad en los delitos contra la propiedad intelectual tras la Ley Orgánica 6/1987, de 11 de noviembre, CFGE nº 2/1989: 675.

La pieza nuclear del software es el programa de ordenador, el cual, lejos de lo que se pueda pensar, no constituye en puridad concepto sinónimo de aquél, sino uno más de los tres elementos que lo integran[54]. Del software forman parte, además, la descripción del programa y el material de apoyo[55], los cuales, no obstante, no constituyen más que accesorios de aquél[56].

En el ámbito penal no existe una posición unánime en el marco de los delitos contra la propiedad intelectual acerca de si se debe otorgar protección a todos los elementos que integran el software o solamente a los programas de ordenador[57]. En cualquier caso, creo que por lo que respecta al acceso ilícito la cuestión se torna bastante clara, pues la propia configuración de la conducta como una introducción de tipo electrónico conduce inexcusablemente a su exclusión.

---

[54] FERNÁNDEZ MASIÁ y ESPLUGUES MOTA, 1996a: 40-41. FERNÁNDEZ MASIÁ y ESPLUGUES MOTA, 1996b: 7.

[55] El origen de esta distinción lo constituye las *Dispositions types sur la protection du logiciel*, cuyo artículo 1, según las cuales:

> **1. Programa de ordenador:** conjunto de instrucciones capaces, cuando se incorporan en un medio técnico legible por el ordenador, de causar que una máquina con capacidad de procesar la información indique, actúe u obtenga una función, tarea o resultado concretos.
>
> **2. Descripción del programa:** una representación procedimental completa en forma verbal, esquemática o de cualquier otro modo, de forma suficientemente detallada para determinar un conjunto de instrucciones que constituyen el programa de ordenador correspondiente.
>
> **3. Material de apoyo:** cualquier material creado para ayudar a la comprensión de un programa de ordenador, como, por ejemplo, las descripciones de un problema o las distintas instrucciones del usuario. OMS, 1978: 9.

[56] FERNÁNDEZ MASIÁ y ESPLUGUES MOTA, 1996a: 41.

[57] La razón que un sector de la doctrina esgrime para excluir su subsunción es el principio de taxatividad: la ausencia de mención expresa a los mismos en el artículo 270, mientras que otros autores no ven ningún género de inconveniente para entenderlos incluidos. DE NOVA LABIÁN, 2010: 147. A favor, GUERRERO ZAPLANA, 2007: 187. MATA Y MARTÍN, 2007: 86-87. GONZÁLEZ RUS, 1999: online. MIRÓ LLINARES, 2004: 89.

1. PROGRAMAS DE ORDENADOR

La determinación de qué debe entenderse por programa de ordenador exige tomar como punto de partida la legislación civil relativa a la regulación de la propiedad intelectual[58], concretamente el Real Decreto Legislativo 1/1996, de 12 de abril, por el que se aprueba el texto refundido de la Ley de Propiedad Intelectual, regularizando, aclarando y armonizando las disposiciones legales vigentes sobre la materia, en adelante Ley de propiedad intelectual[59].

---

[58] La protección del software se articula por medio del derecho de propiedad intelectual y no a través de la propiedad industrial porque el apartado 2 del artículo 52 del Convenio para la Patente Europea, firmado en Munich el 5 de octubre de 1973, excluye expresamente a los programas de ordenador del campo de las invenciones (por tanto, de la regulación relativa a la propiedad industrial y las patentes). Por supuesto, esta exclusión fue reproducida en la norma de transposición de dicha norma, concretamente el artículo 4.2 c) *in fine* de la Ley 11/1986, de 20 de marzo, de Patentes. El motivo principal de esta exclusión se halla en la propia naturaleza jurídica de los programas, los cuales, si bien constituyen una regla del obrar humano, no dan lugar, generalmente, a un producto nuevo mediante la utilización de las fuerzas de la naturaleza, tal y como se exige para que una obra pueda ser considerada industrial. Sin embargo, esta exclusión no es de carácter absoluto, pues el apartado 5 del artículo 4 del mentado Convenio, transpuesto por el artículo 96.3 párrafo 2º de la Ley de Propiedad Intelectual, contempla como excepción aquellos programas que formen parte de una invención patentable. En fin, el artículo 104 de la Ley de propiedad Intelectual permite a los programas gozar de una triple protección simultánea: a través de la propiedad intelectual, que será el derecho de aplicación general, del derecho de patentes, en aquellos casos en los que el programa forme parte de una patente o modelo de utilidad (hardware) y, finalmente, del derecho de marca si es ínsito al título del programa en el Registro de Marcas. Sobre ello MIRÓ LLINARES, 2007: 102-104.

[59] a) Esta que destaca por su alto grado de consolidación debido al amplio desarrollo que este campo ha sufrido a nivel europeo, primero gracias a la aprobación de la Directiva 91/250/EEC del Consejo, de 14 de mayo de 1991, sobre la protección jurídica de programas de ordenador, y, posteriormente, por la Directiva 2009/24/CE del Parlamento Europeo y del Consejo, de 23 de abril de 2009, sobre la protección jurídica de los programas de ordenador, que sustituyó a la anterior. b) Esta norma ha sido modificada recientemente por la Ley 21/2014, de 4 de noviembre, por la que se modifica el texto refundido de la Ley de Propiedad Intelectual, aprobado por Real Decreto Legislativo 1/1996, de 12 de abril, y la Ley 1/2000, de 7 de enero, de Enjuiciamiento Civil.

a) CONCEPTO CIVIL DE PROGRAMA DE ORDENADOR

El artículo 10.1 i) de dicha norma engloba dentro de las obras objeto de la propiedad intelectual a los programas de ordenador, a cuya regulación específica dedica el Título VII del Libro I (artículos 95 a 104). Es el artículo 96.1 el que ofrece una definición de programa informático como t*oda 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*[60].

La Ley extiende la protección de la que gozan los programas también a los contenidos de las distintas etapas de su elaboración y a los demás componentes y elementos que guardan una relación directa con ellos: la documentación preparatoria, la documentación técnica y los manuales de uso (artículo 96.1 párrafo 2º) y las versiones sucesivas y los programas derivados (artículo 96.3)[61].

---

[60] En general la doctrina aglutina en cuatro aspectos básicos las características de los programas de ordenador: MATA Y MARTÍN, 2007: 86. MATA Y MARTÍN, 2006: 104.

1. Funcionamiento: secuencia de instrucciones.

2. Destino: sistema informático.

3. Función o finalidad: realizar una tarea u obtener algún resultado.

4. Soporte: cualquiera que sea su forma de expresión o fijación.

61 Aunque la Ley incluye la documentación preparatoria dentro del propio programa de ordenador, a fortiori parece excluir de esta consideración la documentación técnica y los manuales de uso. Se discute si la protección que otorga la Ley de Propiedad Intelectual se dispensa a todos los elementos de forma unitaria o, por el contrario, a cada uno de los elementos por separado. A tal efecto, la doctrina mayoritaria considera que existen razones fundadas para entender que se trata de una protección única a todo el conjunto, afirmando que la comisión de una infracción contra tan solo una parte del mismo supondría una lesión parcial de los derechos de autor en los delitos contra la propiedad intelectual. MIRÓ LLINARES, 2004: 89. MENDEZ REBOLLAL, 2007: 23.

Una obra intelectual que pretenda obtener protección al amparo de la regulación relativa a la protección intelectual de los programas de ordenador, deberá cumplir, en general, con los mismos requisitos que el artículo 10 prevé para cualquier obra de creación intelectual: por una parte, que se trate de una creación original; y, por otra, que esté expresado en un medio o soporte tangible o intangible.

i) PROGRAMA DE ORDENADOR COMO CREACIÓN ORIGINAL

La primera condición para que un programa de ordenador pueda constituir una obra protegida por la Ley de Propiedad Intelectual es que sea original. En este sentido, el apartado 2 del artículo 96 de la misma establece que *el programa de ordenador será protegido únicamente si fuese original, en el sentido de ser una creación intelectual de su autor*.

La determinación del criterio que debe seguirse para valorar lo que debe entenderse como creación intelectual ha originado mucha controversia en la doctrina civil especializada. En general parece sentir unánime la constatación de una flexibilización del nivel de creatividad exigido en comparación con las demás obras que la Ley protege[62], siendo el principal punto de conflicto la delimitación del punto exacto donde establecer el límite al alcance de dicha flexibilización[63]. Existen dos corrientes al respecto:

[62] LATORRE LATORRE, 2014: 236-237.

[63] LATORRE LATORRE, 2014: 236-237.

a) Criterio de la originalidad subjetiva: un sector de la doctrina considera que el precepto establece un criterio basado en la relación creativa del autor con la obra conforme al cual lo original es aquello que es propio en el sentido de que se ha creado[64]. Desde un punto de vista positivo se trata de que las ideas, el fondo de la obra y los elementos de expresión de ésta estén combinados con el arte de tal forma que el resultado sean obras de personalidad propia diferenciales de las demás[65]. Desde un punto de vista negativo es original todo aquello que no es plagio[66].

b) Criterio objetivo de la novedad de la obra: otro conjunto de autores defiende una versión atenuada del criterio general mantenido para considerar la originalidad de la obra, vinculando el programa al contenido e itinerario informático que se ha seguido para su creación pero no al resultado o utilidad de éste, el cual puede coincidir con el de otros programas también originales (dimensión positiva)[67]. En consecuencia, consideran suficiente que el programa no sea copia exacta de otro y, por tanto, que tenga alguna aportación que haga posible diferenciarlo de otros programas ya existentes (dimensión negativa)[68].

---

[64] LATORRE LATORRE, 2014: 236-237.

[65] Explica GONZALEZ RUS que esta expresión significa que el programa debe ser fruto del esfuerzo intelectual del autor y que, por tanto, no constituya una copia. GONZÁLEZ RUS, 1999: Online.

[66] LATORRE LATORRE, 2014: 235.

[67] MATA Y MARTÍN, 2007: 88.

[68] MIRÓ LLINARES, 2004: 95. MENDEZ REBOLLAL, 2007: 26.

ii) EXPRESIÓN MATERIAL DEL PROGRAMA DE ORDENADOR

Aparte de ser original, para obtener protección al amparo de la Ley de Propiedad Intelectual el programa de ordenador debe estar expresado en algún soporte tangible o intangible. La razón de la anterior radica en el hecho de que, en realidad, no se están protegiendo las meras ideas sino la exteriorización de éstas[69], motivo por el cual se hace necesario el soporte o medio de expresión de las mismas y sus conceptos[70].

Debe diferenciarse, no obstante, exteriorización de materialización, en el sentido de que lo que se exige es que la creación original sea perceptible a terceros, pero no que se encuentre contenida en un determinado soporte[71], por lo que no debe confundirse la propia exteriorización del programa con el medio, instrumento o soporte tangible en el que éste queda fijado, normalmente hardware[72].

---

[69] Como muy bien señala DAVARA RODRÍGUEZ que la protección se realiza sobre la expresión del programa, de forma que lo que se protege no es la propia idea de creación que se encuentra solo en la mente del autor, sino en la representación de ésta, esto es, lo que le permite ser objeto de conocimiento, reproducción o utilización por terceros. Manifiesta LATORRE LATORRE que la obra intelectual es una realidad y no una pura idea, ni un contenido mental ni una abstracción. DAVARA RODRÍGUEZ, 2007: 142. LATORRE LATORRE, 2014: 234.

[70] Resalta GONZALEZ RUS que es muy difícil ofrecer una delimitación clara entre idea y expresión, siendo decisiva para para concretar los términos de tutela y, por tanto, la posibilidad de considerar la existencia de plagio. MATA Y MARTÍN, 2007: 86. GONZÁLEZ RUS, 1999: online.

[71] DE NOVA LABIÁN, 2010: 146. MIRÓ LLINARES, 2004: 89.

[72] Así pues, la forma de expresión es el propio sistema informático, es decir, un conjunto de impulsos o intrusiones eléctricos intangibles, mientras que la forma de fijación sería el medio tangible en el que se graba el programa para su conservación (ROMEO CASABONA). El medio susceptible de contener el programa puede ser diverso siendo el autor quien elige un medio concreto y no otro y organiza dispositivamecte su estructura, que no es sino un signo distintivo de su actividad creativa (LATORRE LATORRE) LATORRE LATORRE, 2014: 234. ROMEO CASABONA, 1988b: 151.

El requisito de la manifestación de la exteriorización de la obra necesaria para su protección no exige ni siquiera que este medio de expresión tenga un carácter tangible, tan solo que sea perceptible o aprehensible por los sentidos[73]. Sin embargo, para que pueda darse esta perceptibilidad será necesario que el programa se registre en un soporte, el cual generalmente será tangible, el cual será diferencial del medio de expresión del programa, esto es, el conjunto de impulsos o instrucciones eléctricos intangibles[74]. Lo anterior conduce a diferenciar el software del hardware o conjunto de elementos físicos que constituyen el ordenador en cuanto tal, y su caracterización como soporte lógico que no se agota en el programa de ordenador, sino que es la última fase de aquél[75].

Podría considerarse expresión de dicha perceptibilidad la interfaz del programa, pues ésta establece la conexión entre el software y el hardware. Esto es lo que suele conocerse como interoperatividad, que puede ser definida como la capacidad de los programas de ordenador para intercambiar información y utilizar mutuamente la información así intercambiada[76]. Sin embargo, tal y como afirma el artículo 96.4 [*n]o estarán protegidos protegidos mediante los derechos de autor con arreglo a la presente Ley las ideas y principios en los que se basan cualquiera de los elementos de un programa de ordenador incluidos los que sirven de fundamento a sus interfaces*.

---

[73] ROMEO CASABONA, 1988a: 1232-1833.

[74] ROMEO CASABONA, 1988a: 1232-1833.

[75] MIRÓ LLINARES, 2004: 89.

[76] LATORRE LATORRE, 2014: 247 nota 24.

b) CONCEPTO PENAL DE PROGRAMA DE ORDENADOR

La definición penal del programa de ordenador parte, por supuesto, de la consideración civil del programa de ordenador[77]. No obstante, la noción de programa de ordenador se extiende a otros elementos relacionados con Internet, que, desde un punto de vista civil, constituyen elementos distintos: las bases de datos y las páginas web.

La razón por la cual la doctrina penal unifica todos estos elementos se debe a que, en principio, todos ellos consisten en una secuencia de instrucciones escritas en un determinado lenguaje informático y que están dotados de un código fuente y un código objeto[78].

---

[77] En general más que la lesión de la propiedad intelectual y la protección de la creación de programas de ordenador como creación intelectual, la protección penal de éstos ha tenido como principal objetivo evitar lo que se ha venido a denominar piratería informática o piratería del software, es decir, la actividad consistente en la realización y distribución de copias ilegales. Esta viene recogida en el artículo 270.6, que castiga a *quien fabrique, importe, ponga en circulación o posea con una finalidad comercial cualquier medio principalmente concebido, producido, adaptado o realizado para facilitar la supresión no autorizada o la neutralización de cualquier dispositivo técnico que se haya utilizado para proteger programas de ordenador o cualquiera de las otras obras, interpretaciones o ejecuciones*. Se trata de un tipo de peligro abstracto que se dirige de forma inmediata a la protección de la propiedad intelectual y de forma mediata a los programas de ordenador, adelantando la barrera punitiva a los actos preparatorios destinados a la desprotección de los programas de ordenador. Podría plantearse la diferenciación entre el acceso ilícito y este precepto, pues en ambos casos se trata de acceder ilícitamente a un programa de ordenador. La diferencia radicará en el elemento subjetivo del injusto que en el ámbito del artículo 270 supondrá ánimo de lucro.
MORETÓN TOQUERO, 2002: 33.

[78] MIRÓ LLINARES, 2005: 176.

2. BASES DE DATOS ELECTRÓNICAS

En el ámbito civil 12.1 de la Ley de Protección Intelectual extiende la protección ofrecida por ésta a las bases de datos que por la selección o disposición de sus contenidos constituyan creaciones intelectual. En este sentido, define como tales las *colecciones de obras, de datos, o de otros elementos independientes dispuestos de manera sistemática o metódica y accesibles individualmente por medios electrónicos o de otra forma*. Sin embargo, en el Derecho civil las bases de datos conforman obras diferenciadas de los programas de ordenador, pues el propio apartado 3 del precepto citado establece que *[l]a protección reconocida a las bases de datos en virtud del presente artículo no se aplicará a los programas de ordenador utilizados en la fabricación o en el funcionamiento de bases de datos accesibles por medios electrónicos*[79].

En el ámbito de los delitos contra la propiedad intelectual, la definición penal de programa informático es extendida en el ámbito penal a las bases de datos electrónicas. Así pues, ambos objetos son incluidos unitariamente como posible objeto material de estos delitos[80].

[79] La Ley de Propiedad Intelectual dedica lo que denomina una protección *sui generis* a las bases de datos, que se contiene en los artículos 133 a 137 de la misma.

[80] MATA Y MARTÍN, 2006: 104. MATA Y MARTÍN, 2007: 88.

3. PÁGINAS WEB

Las páginas web son documentos multimedia interactivos, construidos utilizando cualquiera de los lenguajes de programación reconocidos por los navegadores[81]. Se ha planteado si la página web en sí misma, separada del contenido que la integra, puede ser objeto de los delitos contra la propiedad intelectual[82], en tanto en cuanto su diseño y los múltiples elementos que la integran son creaciones originales[83]. La escasa doctrina que en el ámbito penal se ha pronunciado al respecto responde a la pregunta en sentido afirmativo y, siempre y cuando la página web cumpla los requisitos exigidos por la regulación relativa a la propiedad intelectual, le otorga protección como programa de ordenador sobre la base de que constan de un código fuente y un código objeto[84].

---

[81] MIRÓ LLINARES, 2004: 90.

[82] Acertadamente, MIRÓ LLINARES distingue dentro de una página web tres elementos que, respectivamente, originan tres distintos derechos de propiedad intelectual de naturaleza separada, cada uno de los cuales podrá ser explotado por su correspondiente titular, el cual podrá únicamente autorizar la explotación sobre su derecho.

> **a) Obras de contenido de la página web:** todas y cada una de las distintas obras que forman parte del contenido de la página web serán protegidas de forma separada en atención a su naturaleza.
>
> **b) Página web en sí misma:** viene a integrarse por el conjunto de elementos que, utilizando lenguaje de programación, permiten presentar al autor de la página, mediante la acción conjunta del programa fuente y la lectura del programa objeto por parte del sistema informático, el contenido interactivo.
>
> **c) Diseño del sitio web y presentación visual en pantalla:** se trata de una creación original artística del contenido y de la forma de presentarlo realizada por el diseñador gráfico de la página cuya tutela se articulará a través de una tipología u otra de derechos de la propiedad intelectual en atención a la naturaleza de la obra.

MIRÓ LLINARES, 2004: 90-91. MIRÓ LLINARES, 2005: 176-178.

[83] MIRÓ LLINARES, 2005: 176.

[84] MIRÓ LLINARES, 2004: 90.

B) EL ELEMENTO FÍSICO DEL SISTEMA: HARDWARE

Presentado en el apartado anterior el concepto de software y ofrecida una noción jurídico-penal del mismo, es necesario en este momento ahondar en el concepto de hardware. El hardware viene a integrarse por cada uno de los elementos físicos que integran un sistema informático, los cuales pueden ser múltiples y de variada naturaleza, surgiendo nuevas invenciones cada día. Esta variada naturaleza de los elementos que pueden integrar el hardware del sistema informático así como el hecho de que éste se encuentra en constante evolución impide ofrecer con detalle un catálogo detallado de todos y cada uno de los distintos elementos tangibles que pueden formar parte del sistema informático.

En mi opinión, más que reunir en un cúmulo de páginas todas las innovaciones actuales en la materia[85], me parece lo más oportuno reducir al común denominador estos elementos a los efectos de establecer una base sólida de mínimos sobre los cuales construir el concepto de sistema informático, esto es, determinando cuál es el hardware básico del que debe constar todo sistema informático.

Como hardware básico, todo sistema informático debe constar de tres elementos: un procesador que interprete y ejecute programas,

[85] La protección jurídica del hardware debe articularse a través del régimen jurídico relativo a la propiedad industrial.

una memoria para almacenar datos y programas y un mecanismo para la transmisión de datos desde y hacia el mundo exterior[86].

1. DISPOSITIVOS DE TRANSMISIÓN DE DATOS

Dentro de este elemento se sitúan los mecanismos que permiten introducir los datos en el sistema (dispositivo de entrada) y transmitir el resultado del tratamiento informático al usuario o a otro sistema informático (dispositivo de salida)[87]. Sin embargo, a día de hoy pueden hallarse en el mercado multitud de mecanismos mixtos[88].

---

[86] Aunque en el presente estudio se han agrupado en estas tres categorías, a veces la literatura informática habla de cinco componentes:

a) Elementos de entrada o *inputs*: que son mecanismos a través de los cuales se introduce la información en el sistema, como los teclados o los micrófonos

b) Sección de transformación: que está compuesta por la memoria (bios, drivers, aplicaciones y sistema operativo) y el bus o *datapath*

c) Mecanismo de control: que a veces unido junto con los anteriores se llama procesador o CPU

d) Elementos de salida o *outputs*: que son mecanismos que transmiten el resultado de la informatización de la información al usuario como a través de su presentación al usuario o a otro sistema informático, como los altavoces.

No obstante, en el presente estudio algunos de estos componentes se presentan conjuntamente a los efectos de ofrecer al lector mayor simplicidad en la comprensión de la materia. NULL y LOBUR, 2015: 7.

[87] PATTERSON y HENNSSY, 2014: 16-17.

[88] En la actualidad la más innovadora creación en este ámbito es la pantalla de cristal líquido o LCD. Se trata de una pantalla cuya tecnología consiste en usar una fina capa de líquido de polímero que se puede usar para transmitir o bloquear luz en atención a como es aplicada la carga. PATTERSON y HENNSSY, 2014: 17.

2. MEMORIA

La área de almacenamiento de la memoria es aquella parte del sistema informático en la cual se mantienen almacenados los programas los datos de software y de contenido del sistema[89]. Existen dos tipos de memoria en el sistema informático:

a) Memoria volátil: que almacena datos únicamente si está conectado a una fuente de energía porque el sistema informático se encuentra en marcha[90]. Los datos que contiene son datos de funcionamiento del sistema además de aquellos que los programas necesitan para funcionar mientras éstos están siendo usados[91]. Suele recibir el nombre de memoria primaria o memoria principal[92].

b) Memoria no volátil: una forma de memoria que retiene los datos incluso en ausencia de conexión del sistema a una fuente de energía[93]. Esta segunda memoria recibe también el nombre de memoria secundaria[94].

---

[89] Dentro del procesador se encuentra una pequeña memoria, llamada memoria caché, la cual consiste en una pequeña y rápida memoria que actúa como un buffer para la memoria RAM. Ésta está construida usando una tecnología diferente a la anterior, la memoria estática de acceso aleatorio (static random access memory SRAM). PATTERSON y HENNSSY, 2014: 21-22.

[90]PATTERSON y HENNSSY, 2014: 23.

[91] PATTERSON y HENNSSY, 2014: 23.

[92] Habitualmente ésta es la memoria DRAM. PATTERSON y HENNSSY, 2014: 23.

[93] PATTERSON y HENNSSY, 2014: 22.

94 Las memorias no volátiles más comunes en la actualidad son el disco duro, también llamado disco magnético, que está compuesto de placas rotatorias cubiertas cubiertas con un material de grabación magnético, y la memoria flash, una memoria semiconductora más barata y más lenta que la DRAM pero mucho más cara y rápida que el disco duro. PATTERSON y HENNSSY, 2014: 23.

3. PROCESADOR

Por último, un sistema informático necesitará para su funcionamiento un mecanismo llamado procesador o unidad central de procesamiento (*central processor unit* o CPU). Éste constituye la parte activa del sistema informático, que añade números, test de números, señales de entrada y salida para activar los correspondientes dispositivos de transmisión de datos[95]. La misión principal del procesador es leer las instrucciones y datos los datos de entrada, las procesa y da como resultado datos informático, además de controlar el funcionamiento global del sistema[96]. El procesador está integrado por dos elementos:

> **a) Bus o *datapath:*** es el componente del procesador que realiza operaciones aritméticas[97] de puesta en comunicación de los distintos dispositivos de los que consta el sistema[98].
>
> **b) Control:** es el componente del procesador que dirige el bus, la memoria y los distintos dispositivos de entrada y salida de datos de acuerdo con las instrucciones de un programa informático[99].

---

[95] PATTERSON y HENNSSY, 2014: 19.

[96] El procesador puede cumplir cuatro funciones concretas:

> **a) Memoria a procesador:** leer una instrucción o una unidad de datos de la memoria.
>
> **b) Procesador a memoria:** escribir una unidad de datos en la memoria.
>
> **c) Output/Input a procesador:** leer datos de un dispositivo de entrada o salida.
>
> **d) Procesador a output/input:** enviar datos a un dispositivo de entrada o salida

STALLINGS, 2013: 84.

[97] PATTERSON y HENNSSY, 2014: 19.

[98] STALLINGS, 2013: 85.

[99] PATTERSON y HENNSSY, 2014: 19.

IV. CONTENIDO DEL SISTEMA: RESULTADO DEL PROGRAMA. CRÍTICA

A) OBRA RESULTANTE DEL PROGRAMA

La utilización del software a aplicación conducirá como resultado la transformación de la información introducida como *input* en el sistema para dar lugar a un *output*, que consistirá en la creación de un dato informático[100]. Este *output* en la que consiste la obra resultante del programa no resulta, lógicamente, amparada por el derecho de propiedad intelectual sobre el software, que se proyecta únicamente sobre el propio programa[101]. Así pues, en primer lugar, es necesario distinguir el programa de ordenador de la obra producida por éste, la cual constituye un elemento distinto de éste. El programa es únicamente el instrumento técnico que permite la ejecución de tal resultado.

---

[100] Igualmente por lo que respecta a las bases de datos lo que se protege en el seno de la regulación penal relativa al software es la creación intelectual que pueda constituir la selección o disposición de la materia y no a los datos o la información compilados, cuyo régimen legal deberá ser otro diverso. En este sentido, el articulo 12.1 de la Ley de Propiedad Intelectual establece que su protección se extenderá a las bases de datos que por la selección o disposición de sus contenidos constituyan creaciones intelectuales, sin perjuicio, en su caso, de los derechos que pudieran subsistir sobre dichos contenidos, a los que no resultará extensible dicha protección. MATA Y MARTÍN, 2006: 104.

[101] Afirma LATORRE LATORRE que la obra creada por ordenador en sí misma no existe, pues ésta se repetirá cuantas veces se ponga en ejecución el programa, que es quien la identifica y le otorga el rasgo de originalidad y no el resultado de la ejecución de éste, pues igualmente por programas distintos. En este sentido, considera el autor que la obra creada por el ordenador no existe separadamente del programa. Sin la presencia del programa es de total imposibilidad la creación y también el programa carece de sentido si no mantiene vocación de creación. LATORRE LATORRE, 2014: 250.

Además, la utilización de programas de distinta naturaleza dará lugar a distintas creaciones que no siempre conformarán obras de protección conforme a los derechos de propiedad intelectual. En el caso de que tal resultado de lugar a una obra intelectual, ésta recibirá protección de forma independiente al programa[102]. Pero es posible también que la tutela penal del resultado del programa se articule conforme a cualquier otro derecho[103].

Los distintos datos informáticos creación de los programas irán almacenándose en el sistema e irán conformando el contenido del sistema informático[104], el cual conforme a las consideraciones efectuadas en el presente capítulo resulta perfectamente diferenciable de los elementos que integran el sistema informático. A tal efecto, éste quedará también excluido del ámbito típico del acceso ilícito y, si se produce cualquier agresión contra el mismo, ésta tendrá que ser castigada separadamente conforme al tipo delictivo correspondiente.

---

[102] Véase Apartados precedentes de la presente Sección.

[103] El sistema informático puede contener datos relativos a la intimidad de las personas, al secreto de las comunicaciones, a la imagen, al secreto de empresa, a la seguridad nacional, información económica, etc. Véase Sección 1ª del presente Capítulo.

[104] Refleja de forma clara esta función la doctrina y la jurisprudencia italiana al establecer que el sistema tiene como función última el registro o almacenamiento de información por medio de impulsos electrónicos a través de la creación de datos elaborados automáticamente por la máquina como consecuencia de la introducción de símbolos (bit) números (códigos) en combinación diversa. Estos datos elaborados automáticamente por la máquina general la información que constituye un conjunto más o menos extenso de datos organizados según la lógica que consienta la propia atribución de un significado para el usuario. Caracteriza la noción de sistema informático: la elaboración automática de datos AMORE et al., 2006: 97-98. CUOMO y RAZZANTE, 2009: 94-95. DELPINO, 2003: 584.

B) ACCESO AL SISTEMA COMO ACCESO A DATOS

Al hilo de lo anterior podría plantearse la cuestión de si la conducta de acceso ilícito a un sistema informático no implica en sí misma acceso a datos, ello teniendo en cuenta que el elemento diferencial del propio sistema informático es el software y que éste no consiste más que en un conjunto de datos que viabilizan el funcionamiento del sistema[105]. Pues bien, habiendo definido el acceso al sistema como introducción electrónica en el mismo, esto es, en el software del sistema, sería posible sobreentender de esta afirmación que acceder al sistema ya es acceder a datos, tal y como de hecho considera cierto sector doctrinal[106].

La respuesta no es baladí porque no son pocos los Estados que han optado por proteger los datos informáticos en lugar del sistema informático[107], y la opción por una u otra solución determina concluir la necesidad de reforma de sus respectivas legislaciones penales por inadecuación a la normativa supranacional.

---

[105] PATTERSON y HENNSSY, 2014: 14.

[106] Defienden algunos autores que en el momento en que un sujeto se introduce a un sistema informático o telemático, éste se está automáticamente introduciendo en datos, produciéndose siempre la adquisición cognitiva de datos contenidos en el sistema en el momento en que éste realiza las distintas operaciones que el accidente le solicita. Como muy bien indica FROSINI, cada vez que un sistema informático entra en contacto con otro sistema informático o telemático, automáticamente sucede una especie de adquisición-cognición de datos contenidos en el sistema en cuanto la máquina registra necesariamente algunos datos relativos a la operación realizada en el sistema externo ATERNO, 2000: 2990. FROSINI, 2000: 2990. ¿?

[107] Ésta es la opción que siguió la Ley Orgánica 5/2010, de 22 de junio, que incriminaba el acceso a datos y programas informáticos contenidos en todo o en parte de un sistema informático. Además, entre los países signatarios del Convenio que recogen como objeto material los datos informáticos se encuentran Alemania, Australia, Bulgaria, Dinamarca, Georgia, Grecia, Islandia, Malta, Moldavia, Noruega y Rusia; si bien Bélgica, Bosnia y Herzegovina, Croacia, y Finlandia ofrecen tutela tanto a los sistemas como a los datos. (última consulta: 09.2015)

Creo que el *quid* de la cuestión se halla en la interrelación del propio concepto de dato informático con el de sistema. Así pues, tanto el Convenio sobre Cibercrimen de Budapest, de 23 de noviembre de 2001, y la Directiva, 2013/40/UE, de 12 de agosto de 2013, del Parlamento Europeo y del Consejo, relativa a los ataques contra los sistemas de información y por la que se sustituye la Decisión marco 2005/222/JAI del Consejo.

Recordando la definición de datos informáticos que efectúan ambas normas: *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*, creo que conforme a esta definición son posibles dos interpretaciones:

> **a) Concepto amplio de dato informático:** englobar dentro de dicha noción cualquier representación informática relativa al procesamiento automatizado, lo que implicaría entender comprendidos en esta definición tanto el conjunto de datos que integra el software, como el conjunto de datos que conforma el contenido del sistema.
>
> **b) Concepto restringido de dato informático:** supone restringir el concepto de dato a la información que en tanto *input* se introduce en el sistema informático a los efectos de su procesamiento automatizado y la obtención de un dato informático *output* calificable como dato de contenido del sistema, esto es, como obra resultado de la ejecución del programa.

La primera parece ser la opción a la que se ha acogido la § 202a (2) del Código penal alemán, que define dato informático como aquellos que se almacenan o transmiten en forma electrónica, magnética o de otra manera en forma no inmediatamente perceptible[108], y que no contenta en absoluto a la doctrina alemana. Ésta considera que la definición que contiene la Sección transcrita es excesivamente abierta[109] (la única característica definitoria de los datos es el hecho de ser o estar siendo transmitidos o almacenados de una forma no directamente perceptible) y le ha atribuido un valor muy escaso, al entender que conforme a ella no es posible identificar cuáles son los datos a los que se ofrece protección[110], siendo que ofrece protección a todo tipo de datos[111] y de cualquier formato[112].

---

[108] § 202a Ausspähen von Daten (2) *Daten im Sinne des Absatzes 1 sind nur solche, die elektronisch, magnetisch oder sonst nicht unmittelbar wahrnehmbar gespeichert sind oder übermittelt werden*.

[109] ALTENHAIN y WIETZ, 2013: párrafo 2. FISCHER, 2013: 1395 párrafo 2. GRAF, 2012: 181 párrafo 12. HILGENDORF, 2005: 1442 párrafo 7. HOYER, 2012: 3 párrafo 3 (Abschnitt 15). KARGL, 2013: 1407 párrafo 4. KINDHÄUSER, 2013: 1819. HEGER, 2014: 965 o párrafo 2. LENCKNER y EISELE, 2010: 1820. TAG, 2013: 1091 párrafo 4. WEIDEMANN, 2010: 1307 párrafo 4.

[110] Uno de los principales puntos objeto de crítica, según se ha expuesto en el capítulo correspodiente, ha sido su excesiva generalidad. En este sentido, se aduce que se trata de una enunciación genérica que resulta aplicable a cualquier ámbito del Derecho sin que aporte nada en particular a la descripción del tipo, al no poderse establecer una relación directa con él (BOSCH, KARGL). La razón principal para ello se centra en que la noción legal de dato no aparece claramente delimitada en la norma de una manera positiva sino únicamente a través de una limitación del concepto por medio de la exigencia de características adicionales (ALTENHAIN und WIETZ, GRAF, KARGL, TAG). De hecho, el único aspecto positivo que la doctrina alemana vincula a la definición es el de su apertura a los nuevos avances de la tecnología. ALTENHAIN y WIETZ, 2013: párrafo 2. BOSCH, 2014: 1275 párrafo 2. GRAF, 2012: 180-181 párrafo 10. KARGL, 2013: 1407 párrafo 4. TAG, 2013: 1091 párrafo 4.

[111] ALTENHAIN y WIETZ, 2013: párrafo 2. BOSCH, 2014: 1275 párrafo 2. FISCHER, 2013: 1395 párrafo 2. GRAF, 2012: 180-181 párrafo 10. HEGER, 2014: 965 o párrafo 2. HILGENDORF, 2005: 1442 párrafo 7.

[112] KARGL, 2013: 1407 párrafo 4.

En cambio, no sin ciertas dudas, a la conclusión opuesta debía llegarse en relación con el hoy derogado apartado 3 del artículo 197 introducido por la Ley Orgánica 5/2010, de 22 de junio, que adoptaba como objeto material del acceso ilícito a un sistema informático *los datos y programas informáticos contenidos en todo o en parte de un sistema informático*[113], pues el artículo 197 del Código penal conformaba un tipo residual de los restantes apartados del precepto cuyo ámbito típico debía fijarse en atención a una delimitación sistemática negativa[114].

---

[113] La Ley Orgánica 5/2010, de 22 junio, introdujo el acceso ilícito en el apartado 3 del artículo 197 del Código penal como un tipo de equivalencia en relación con el delito de descubrimiento y revelación de secretos. Al igual que en los demás apartados del precepto, el objeto material del delito eran los datos, a los que en este caso se les atribuía como única característica que se hallaran contenidos en todo o en parte de un sistema informático. En mi opinión, aunque con tal expresión el legislador pretendía concretar el concepto de dato en la redacción típica y, con ello, deslindarlo de los datos que hallaban protección por medio de los demás párrafos, en realidad se trataba de dos notas que no aportaban demasiado:

> **a) Datos contenidos en un sistema informático:** cabía preguntarse si sería posible encontrar un dato que fuera informático y que no se hallara contenido en un sistema informático, puesto que pueden existir datos que no tengan la característica de informáticos y que sí se encuentren fuera del sistema informático, pero precisamente lo que caracteriza a los datos informáticos es que estén contenidos en el sistema informático. En consecuencia, a mi modo de ver, el inciso contenidos en un sistema informático resultaba totalmente prescindible porque no aportaba nada a la delimitación de cuáles eran los datos que debían entenderse englobados en el apartado 3 del artículo 197, siendo una reiteración superflua de la idea de dato informático.
>
> **b) Datos contenidos en todo en parte del sistema:** tampoco podía considerarse como un aspecto relevante de la definición de dato, por una parte, porque todos los datos se hallan contenidos en una parte del sistema sin que ello sea algo sustancial para definirlos, por otra, porque afirmar que un solo dato puede contenerse en todo el sistema informático me parece absolutamente exagerado y materialmente imposible.

[114] Véase Sección 1ª de este Capítulo.

Creo que lo más acertado es decantarse por la segunda de las definiciones, esto es, el concepto restringido de dato, y en este sentido me uno a la doctrina alemana apuntada al entender que la definición de dato informático no puede darse la máxima amplitud[115] de tal forma que al amparo de la misma se ofrezcan cobertura a todos los ataques contra los mismos, pues ello iría en contra del carácter fragmentario y de *ultima ratio* que debe atribuirse al Derecho penal.

También rozaría un precepto genérico que castigara el acceso genérico a cualquier posible dato que se encontrase en el sistema el mandato de certeza que impone el principio de taxatividad ya que los ciudadanos no podrían conocer con extrema claridad la norma conforme a la cual adaptar su conducta, siendo el margen dejado al arbitrio judicial excesivamente amplio. Es cierto que el lenguaje de la programación utiliza instrucciones y datos para hacer funcionar a un sistema informático[116]. Sin embargo, este lenguaje es común a todos los sistemas informáticos y debe distinguirse de los datos contenidos en el sistema[117]. Por este motivo, no me parece adecuado poner al mismo nivel una y otra clase de datos.

Deben diferenciarse a mi juicio dos niveles: el relativo al contenido del sistema informático y el relativo al continente, el sistema. Los datos relativos al sistema informático deben protegerse teniendo en cuenta el todo que conforma el propio sistema y no al margen de este. No me aparece adecuada una protección parcial sino que la protección debe ofrecerse al todo, al conjunto que constituye el

---

[115] ALTENHAIN y WIETZ, 2013: párrafo 2. BOSCH, 2014: 1275 párrafo 2. GRAF, 2012: 180-181 párrafo 10. KARGL, 2013: 1407 párrafo 4. TAG, 2013: 1091 párrafo 4.

[116] Los distintos elementos que integran el sistema informático interaccionan entre ellos por medio de lo que se denomina lenguaje de programación, que puede dividirse entre lenguaje de alto nivel (el que utiliza el software) o lenguaje básico o del hardware, un conjunto de señales eléctricas y que utiliza únicamente 0 y 1, conocido como código binario o bit. La combinación de estos números hace comportarse al sistema de una u otra manera, llamándose las distintas combinaciones comandos y que cuando se unen crean lo que se denomina instrucciones, que son solo colecciones de bits que el sistema entiende y obedece.

[117] Véanse los dos primeros apartados de esta Sección.

sistema. La definición de sistema informático se agota en los conceptos de software y hardware y considero cierto el hecho de que como se ha dicho que el programa consiste en una secuencia de instrucciones, esta secuencia de instrucciones no son más que comandos que el hardware entiende y obedece[118].

Por las razones expuestas, aunque ciertamente, la conexión al sistema ya implica en sí mismo el acceso a un género de datos que podrían llamarse informáticos, no puede equipararse esta acción a la de acceso al contenido, pues tiene un injusto menor acceder a aquellos datos que sirven como base para el funcionamiento del sistema. Ello es necesario para introducirse en la memoria interna del sistema, se trata de datos de carácter simbólico y sintético diferentes de los documentos, datos y programas que son contenidos en el sistema informático[119]. Al margen de la seguridad informática, de ello no resulta la afectación para ningún bien jurídico[120].

---

[118] PATTERSON y HENNSSY, 2014: 14.

[119] PECORELLA, 2006: 336.

[120] El conocimiento de algunos datos resulta inevitable en todos y cada uno de los supuestos de acceso ilícito, pues para lograr el acceso al sistema se tiene que haber accedido a datos, ya que el sistema informático está integrado por datos PECORELLA, 2006: 336.

C) VALORACIÓN PERSONAL

En tanto en cuanto el acceso ilícito se ha definido como una introducción electrónica en el capítulo correspondiente a la conducta típica[121], no podrá considerarse la mera introducción en el hardware del sistema informático no podrá considerarse típica a los efectos del acceso ilícito, pues el hardware no constituye más que un elemento accesorio del software, el cual es el efectivo motor del sistema informático.

Siempre que un instrumento tecnológico conste de un procesador una memoria y uno o más dispositivos de entrada y salida, con independencia de la tipología de estos, podremos decir que estamos ante un sistema informático.

Como hardware básico, todo sistema informático debe constar de tres elementos: un procesador que interprete y ejecute programas, una memoria para almacenar datos y programas y un mecanismo para la transmisión de datos desde y hacia el mundo exterior[122].

---

[121] Véase Capítulo IV.

[122] Aunque en el presente estudio se han agrupado en estas tres categorías, a veces la literatura informática habla de cinco componentes:

> **a) Elementos de entrada o *inputs***: que son mecanismos a través de los cuales se introduce la información en el sistema, como los teclados o los micrófonos
>
> **b) Sección de transformación:** que está compuesta por la memoria (bios, drivers, aplicaciones y sistema operativo) y el bus o *datapath*
>
> **c) Mecanismo de control:** que a veces unido junto con los anteriores se llama procesador o CPU
>
> **d) Elementos de salida o *outputs*:** que son mecanismos que transmiten el resultado de la informatización de la información al usuario como a través de su presentación al usuario o a otro sistema informático, como los altavoces.

No obstante, en el presente estudio algunos de estos componentes se presentan conjuntamente a los efectos de ofrecer al lector mayor simplicidad en la comprensión de la materia. NULL y LOBUR, 2015: 7.

Sin embargo, aunque un sistema para ser caracterizado como informático deba integrarse de los elementos mencionados, lo que caracterizará efectivamente el delito de acceso ilícito no es la introducción en el hardware sino la introducción electrónica en el sistema, lo que implica necesariamente la iniciación de algún tipo de diálogo con en el software del sistema. Será atípica, por tanto, la mera introducción en el hardware, salvo en aquellos supuestos en los que integre tentativa del delito.

CAPÍTULO VI
MEDIOS COMISIVOS DEL DELITO, EN ESPECIAL, LA VULNERACIÓN DE LAS MEDIDAS DE SEGURIDAD ESTABLECIDAS PARA IMPEDIR EL ACCESO

I. INTRODUCCIÓN

El artículo 197.1 *bis* comienza con el inciso *[e]l que, por cualquier medio o procedimiento y vulnerando las medidas de seguridad establecidas para impedirlo* haciendo alusión a los medios comisivos a través de los cuales debe ser realizada la acción. Según dicha literalidad, lo que es una pretensión de amplitud e indeterminación de la forma de ejecución del hecho, se restringe con la previsión de una modalidad específica de realización del tipo a unos medios comisivos determinados. Así, a pesar de que en un principio da la impresión de que se trata de un tipo de estructura abierta: por cualquier medio, acto seguido se percibe que, en realidad, es un tipo de estructura cerrada: vulnerando medidas de seguridad.

No obstante, antes de llegar a una conclusión excesivamente apresurada, se presenta como ineludible un análisis detenido de este inciso, examinando su contenido material para poder después valorar conforme a ello la necesidad de su inclusión en el tipo. Concluido lo anterior, será posible ofrecer una mayor concreción en el estudio del elemento de las medidas de seguridad, definiendo qué debe entenderse como tales, su contenido y tipología y, por último, qué implica la vulneración de éstas para la realización del tipo delictivo.

Una vez establecidos los parámetros anteriores, podrá precisarse con claridad cuál es la vinculación existente entre ambos y, así, resolver las dudas existentes acerca de la adecuación de la descripción típica. A todo ello es a lo que se dedican las páginas de este Capítulo.

II. EL INCISO *POR CUALQUIER MEDIO O PROCEDIMIENTO*

La redacción del artículo 197.1 *bis* se inicia con el inciso *por cualquier medio o procedimiento*. Señala FERNÁNDEZ TERUELO que con ello lo que se pretende es acentuar la relevancia del resultado de la acción por encima de los medios de comisión[1]. Es cierto que *a priori* dicho precepto parece no limitar las posibles modalidades de la acción, siendo suficiente con que éstas sean idóneas para la producción del resultado. Sin embargo, en realidad el acceso ilícito no es un delito resultativo, ya que la indeterminación de medios comisivos no es tal. Esta expresión debe ser puesta en relación con el siguiente elemento al que se refiere el precepto. Así pues, acto seguido el artículo 197.1 *bis* establece que el delito debe cometerse *vulnerando las medidas de seguridad establecidas para impedirlo*. Esta expresión exige que la realización del tipo tenga lugar únicamente de la forma enunciada y convierte el delito previsto en el artículo 197.1 *bis* en un tipo de estructura cerrada, es decir, en un delito de medios determinados que únicamente puede cometerse a través de un solo procedimiento: la superación de los medios de protección establecidos para impedir el acceso.

No es la primera vez que se ponen en relación ambos elementos típicos, pues ROMEO CASABONA ya había establecido una vinculación entre ellos en el seno del apartado 2 del artículo 197. Este precepto recoge, entre las distintas modalidades típicas, la conducta de acceso[2], determinando que éste puede realizarse *por cualquier medio* aunque sin aludir directamente a las medidas de seguridad. Dicho autor entiende que tal expresión debe interpretarse en el sentido de que el sujeto activo debe haber superado algún mecanismo de protección para cometer el acceso, admitiendo al efecto tanto la superación de medios físicos como lógicos[3].

---

[1] FERNÁNDEZ TERUELO, 2011: 195.

[2] Sobre la conducta de acceso en este apartado véase Capítulo IV.

[3] Hace referencia al engaño del empleado encargado o responsable del fichero o a procedimientos telemáticos desde otro terminal. ROMEO CASABONA, 2004: 121. Opina, en cambio, que expresa el quebranto de la reserva JAREÑO LEAL, 2008: 32.

Esta postura, que me parece excesivamente restringida como criterio hermenéutico para el apartado 2 del artículo 197, en el que si bien la vulneración de medidas de seguridad constituirá una de las formas más frecuentes de comisión del delito, cabe también entender amparado en el tipo penal cualquier otro acceso que se produzca a través de cualquier otra vía distinta.

Lo anterior hace necesaria la búsqueda de una significación distinta para esta expresión y, en caso de que ello no sea posible, concluir que no aporta nada a la descripción típica al quedar perfectamente enmarcada la conducta por la vulneración de medidas de seguridad. Sin negar que se trate de una expresión que no resulta terminante para la interpretación del tipo, considero junto a MORALES PRATS que tal pretensión de globalidad quiere indicar que el tipo puede quedar colmado por todo tipo de conductas que permitan el acceso, desde la captación visual y física por contemplar el sistema informático hasta los acceso más sofisticados que proporciona la conexión electrónica a través de otro sistema[4].

En consecuencia, en el plano fáctico dicha expresión viene a ser indicativa, en mi opinión, no de que se deben vulnerar medidas de seguridad para cometer el acceso, sino de que caben cualquiera de las dos posibles vías que en la práctica existen para introducirse en un sistema informático, que son analizadas en otra parte del presente estudio[5]:

> **a) Acceso físico:** el acceso a la localización espacial donde éste se encuentra y posterior acceso físico al sistema.
>
> **b) Acceso lógico:** el acceso remoto cometido a distancia desde otro sistema informático conectado a una red privada de área local o a una red pública global (Internet).

---

[4] MORALES PRATS, 2011: 484.

[5] Véase Capítulo IV Sección 2ª Subsección 2ª.

III. VULNERACIÓN DE MEDIDAS DE SEGURIDAD

El artículo 197.1 *bis* prevé como uno de los elementos de la parte objetiva de la conducta típica la vulneración de las medidas de seguridad establecidas para impedir el acceso o el mantenimiento en el sistema.

El Código penal español, siguiendo a la mayor parte de países[6], optó ya en 2010 por introducir en la transposición una de las exigencias de carácter potestativo que disponía el Convenio sobre Cibercrimen de 2001[7] y la única prevista en la Decisión Marco 2005/222/JAI del Consejo, de 24 de febrero, relativa a los ataques contra los sistemas de información[8].

Ésta, además, ha sido mantenida en la reforma operada en 2015 en coherencia con 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, la cual incluyó a la vulneración de medidas de seguridad entre los elementos del tipo a introducir con carácter preceptivo en la descripción típica del delito[9].

---

[6] Véase Capítulo I. Apartado X.

[7] Cabe recordar que el Convenio de Cibercrimen preveía como elementos preceptivos únicamente la conducta base, esto es, el acceso a todo o a parte de un sistema informático. A parte de ello, se preveían cuatro elementos potestativos que los Estados podían introducir para restringir la conducta: dos en la parte objetiva del tipo: la vulneración de las medidas de seguridad y la interconexión de los sistemas; y dos en relación con el tipo subjetivo: la inclusión como elemento subjetivo del tipo o bien la finalidad de obtener datos informáticos o bien la consecución de cualquier otro fin deshonesto en atención a la realidad criminal de los Estados. Teniendo en cuenta este dato, se pone de manifiesto que el Código penal español solo ha introducido una de las cuatro posibilidades que contemplaba el Convenio: la vulneración de las medidas de seguridad. Para ulteriores cuestiones respecto de esta temática véase el apartado Véase Capítulo I. Apartado VI.

[8] Véase Capítulo I. Apartado VIII. Letra B)

[9] Véase Capítulo I. Apartado VIII. Letra C)

La introducción de este elemento típico tiene importantes consecuencias desde diferentes puntos de vista:

a) Para la aplicación del precepto, suponiendo la restricción de los supuestos subsumibles en el mismo, más aún cuando según parece desprenderse del tenor literal está vinculado también a la conducta de mantenimiento;

b) Para la determinación de la forma de ejecución del hecho, siendo necesario determinar qué debe entenderse por medida de seguridad y cual es su contenido y tipología;

c) y, por último, para la consumación del delito, siendo que la vulneración de las medidas de seguridad marcará el hito fundamental de ésta.

A) RESTRICCIÓN DEL ÁMBITO APLICATIVO

1. CONSECUENCIAS

La tipicidad de la conducta se encuentra limitada a la vulneración de medidas de las seguridad establecidas para impedirlo. La protección penal del acceso ilícito a un sistema informático se encuentra limitada, por tanto, a los sistemas protegidos por medidas de seguridad. Este hecho conduce a la introducción de importantes restricciones en el ámbito aplicativo del precepto, actuando como un criterio de selección de la tutela penal[10], que se halla limitada únicamente a los sistemas informáticos o telemáticos protegidos por medidas de seguridad, quedando fuera del ámbito típico todos aquellos que no dispongan de tales medidas[11].

1. La primera cuestión a comentar debe centrarse en la finalidad de este elemento. Cierto sector de la doctrina comparada lo vincula a la voluntad del titular, afirmando que se trata de la manifestación explícita de la ausencia de conformidad de éste con la realización de la conducta[12]. En este sentido, se equipara dicha expresión a la condición requerida en el delito de allanamiento de morada de que el hecho se realice en contra de la voluntad expresa o tácita del titular[13]. Sin negar que hasta cierto punto ésta conforma un reflejo muy indirecto de dicha voluntad, no puedo compartir esta idea por los motivos que procedo a señalar:

---

[10] PECORELLA, 2011: 5983.

[11] Véase este Capítulo Apartado III. C)

[12] GONZÁLEZ RUS, 2011: 520. SÁNCHEZ DOMINGO, 1998: 39. CADOPPI et al., 2011: 533. TRENTACAPILLI, 2002: 1283. MAIORANO, 2010: 1360. En este sentido se pronuncia también un sector de la jurisprudencia italiana. Véase, por ejemplo, la Cass. pen. Sez. V 00/ 12732.

[13] Afirman DESTITO Y DEZZANI que para poderse hablar de domicilio informático en tanto espacio de pertenencia exclusiva del sujeto con prohibición de la intrusión de otros sujetos sin autorización específica y expresa del titular, en el sentido exigido por el tipo, es necesario que ésta sea patente e inequívoca en cuanto a la exclusión de terceros, hecho al que contribuye la previsión de la vulneración de medidas de seguridad. DESTITO et al., 2007: 83.. PICA, 1999: 43..

a) Confusión de términos: Tal afirmación supone confundir una parte esencial del tipo como es la voluntad del sujeto pasivo con los medios comisivos del delito, siendo que ambos constituyen elementos autónomos. Lo anterior se confirma en tres ideas:

a.1) Objeto: La voluntad disconforme del titular con la conducta realizada altera el injusto o bien en el sentido de justificar el hecho convirtiéndolo en legítimo[14], o bien, en caso contrario, en el de garantizar la subsistencia del delito[15]. A ello se refieren precisamente los incisos *sin la debida autorización* y *en contra de la voluntad de quien tenga el legítimo derecho a excluirlo*[16]. No obstante, lo anterior no significa que no exista voluntad del titular contraria al acceso en aquellos sistemas que no disponen de medidas de seguridad[17], aunque tal acceso jurídico-penalmente no sea un acto típico[18]. De hecho, creo que la voluntad contraria es obvia y la decisión de no proteger al titular del sistema que no ha instalado mecanismos de seguridad no es determinante para la tipicidad o la antijuridicidad, sino que responde a razones de política criminal[19].

---

[14] Véase Capítulo VII.

[15] PECORELLA, 2011: 5983.

[16] En un sentido similar, solo que desde la perspectiva del consentimiento DESTITO et al., 2007: 87. PICA, 1999: 43.

[17] PICA, 1999: 44. TOMÁS - VALIENTE LANUZA, 2010: 803.

[18] Puede establecerse en este aspecto un claro paralelismo entre este delito y los de hurto y robo. Así pues, lo que se castiga con más pena en el robo no es la realización de la conducta en contra de la voluntad del titular sino la utilización de una especial intensidad en los medios comisivos. Como muy bien indica MATA Y MARTÍN, el hurto constituye el delito base para el delito de robo, solo que *en tal caso no existe la necesidad de sobrepasar ninguna barrera* de protección, pues *se trata de una actuación clandestina, en la que de estar presente una voluntad opuesta a la sustracción ésta no se encuentra exteriorizada*. Por todos, MATA Y MARTÍN, 2011: 922..

[19] Llama la atención cuanto menos que en este delito el legislador haya adoptado una posición más restriccionista que extensiva del ámbito de lo punible, ello teniendo en cuenta la corriente expansionista que impera hoy en el Derecho penal de nuestro país. En efecto, la intervención penal está hoy liderada por el dogma de la punición y de la desformalización tendente a la creación de tipos penales de carácter ambiguo que no permiten deducir el ámbito de lo que realmente debe ser típico sino tras un prolijo e ingente esfuerzo hermenéutico carente a su vez de seguridad jurídica. ALBRECHT, 2000: 483.. SILVA SÁNCHEZ, 2001: 21..

a.2) Naturaleza: Mientras que la autorización tiene una naturaleza inmaterial, las medidas de seguridad tienen carácter físico[20]. Así, la autorización es una manifestación de la voluntad o actitud de un sujeto frente a un determinado hecho, mientras que las medidas de seguridad conforman elementos materiales cuya misión principal es ofrecer protección a un contenido excluyendo a los terceros ajenos al mismo[21].

a.3) Ámbito procesal: la vinculación de este elemento a la voluntad del titular del sistema supondría el establecimiento de una presunción *iuris et de iure* de que, vulneradas las medidas, la conducta es típica por falta de autorización del titular. Esta idea elimina, por tanto, la efectiva comprobación de si, aun a pesar de haberse superado algún tipo de medida de seguridad, hubo conformidad del propietario con el comportamiento realizado por parte del sujeto activo, estableciéndose así una suerte de responsabilidad objetiva[22]. La concurrencia de la autorización y de la tipicidad subjetiva debe examinarse en todo caso, siendo de todo punto inaceptable el establecimiento de un juicio presuntivo sobre la voluntad e intención del sujeto activo o del propio pasivo[23].

---

[20] CANNATA, 2006: 533.. PICA, 1999: 43..

[21] Véase Capítulo VII.

[22] PICA, 1999: 47..

[23] Afirma PICA que la falta de voluntad del propietario del sistema siempre debe comprobarse, aunque resulte claro que el acceso ha tenido lugar vulnerando los mecanismos de protección, ya que la existencia de los elementos objetivos del tipo no exime la comprobación de la concurrencia parte subjetiva de la tipicidad: más aún cuando el legislador italiano ha previsto expresamente la exigencia de que la conducta se realice abusivamente contra la autorización expresa o tácita de quién tiene el derecho a excluir de acceso. A tal efecto, considera requisito ineludible la verificación de la disidencia del titular a los efectos de poner de relieve la efectiva presencia o ausencia de consentimiento a favor o en contra de la comisión del hecho. PICA, 1999: 47 y 48..

b) Criterio preponderante: Entender que la exigencia de vulneración de las medidas de seguridad tiene como fin único la exteriorización de la autorización implica *a sensu contrario* presumir *iuris tantum* que existe conformidad al acceso en todos aquellos sistemas que no disponen de medidas de seguridad, algo que no es verdad[24]. Es más, en el delito de allanamiento de morada, doctrina y jurisprudencia coinciden en que el mero hecho de que la puerta esté abierta no puede ser interpretado como una voluntad favorable de carácter tácito a la posible entrada de cualquier extraño[25].

Habiendo descartado la tesis anterior, no voy a proceder ahora a analizar cuál es la finalidad que cumplen las medidas de seguridad respecto del sistema. Baste por el momento decir que éstas tienen por objeto dos funciones: impedir el libre acceso de terceros al sistema[26] y procurar la reservar del contenido[27] porque de ello me ocuparé más tarde al requerir antes mi atención otra cuestión. Así pues, negar la vinculación de tales medios a la voluntad del titular del sistema y, con ello, eliminar la absoluta transcendencia que tal vinculación significa para este elemento a los efectos de la subsistencia del delito, conduce a plantearse hasta que punto su referencia resulta ineludible y hasta donde llega la restricción del ámbito aplicativo del precepto como consecuencia de su mención.

---

[24] PICA, 1999: 43.

[25] Afirma muy acertadamente CUOMO que las medidas de seguridad se comportan en el entorno informático como a de la perimetración mural o la delimintación espacial connatural al domicilio tradicional para la tutela de los bienes jurídicos como el patrimonio, la privacidad, la fe pública, la inviolabilidad del domicilio o la libertad individual. CUOMO y RAZZANTE, 2009: 98..

[26] A favor, AMORE et al., 2006: 100.. CARINGELLA et al., 2010: 1052-1053.. MONACO, 2011: 2334. CATULO, 930. D'AIETTI, 1994: 74. PECORELLA, 2011: 5983. FIANDANCA y MUSCO, 2013: 294. MUCCIARELLI, 1996: 99. PICOTTI, Studi di Diritto penale, 114.

[27] PECORELLA, 2011: 5983. A favor ALMA y PERRONI, 1997: 505. BORRUSO et al., 1994: 28.. CERQUA, 2000: 53. CUOMO y IZZI, 2002: 1021. MANTOVANI, 2011: 518-521. TRENTACAPILLI, 2002: 1283. Relazione di presentazione dello Schema di Progetto di legge contenente modificazioni ed integrazioni delle norme del Codice penale in tema di criminalità informática, Documenti Giustizia, 1991, n. 9, 142 y ss.

2. LA INCLUSIÓN DEL INCISO VULNERACIÓN MEDIDAS DE SEGURIDAD

En la medida en que la exigencia de cometer el hecho vulnerando medidas de seguridad supone una restricción de la conducta típica, se impone como necesario analizar si tal limitación de los supuestos subsumibles resulta coherente con el fin de protección de la norma. En este sentido, lo primero que debe reseñarse es que la decisión acerca de si debe ofrecerse tutela también a los sistemas que carecen de medidas de seguridad es una decisión de política criminal que depende, a mi juicio, de la realidad criminal de cada país[28]. Se trata, no obstante, de una decisión de trascendencia máxima, ya que, como muy bien pone de relieve CUOMO, la adopción de medidas de seguridad se ha convertido *a sensu contrario* en una obligación legal cuya violación es penalmente sancionada con la ausencia de repercusión penal de cualquier conducta realizada contra un sistema que no disponga de ellas[29].

---

[28] En el ámbito italiano pueden encontrarse opiniones para todos los gustos. Aquel sector doctrinal que considera que éstas constituyen la expresión del consentimiento se manifiesta, en coherencia, a favor de su previsión típica. En contra, se argumenta que supone una penalización excesiva e irracional del ámbito aplicativo de la norma que contrasta con la finalidad de la tutela de ésta. Se afirma que en el acceso ilícito se exige, a diferencia de lo que ocurre en el allanamiento de morada (a imagen y semejanza del que se ha construido el acceso ilícito en este ordenmiento) además de la afirmación de la necesidad del disenso del titular, una calidad concreta, física, de los bienes objeto material de la acción (el sistema informático), cuál es la presencia de medidas de seguridad, con lo que se están dejando demasiados e injustificados espacios de libertad a las conductas de acceso ilícito, y poniendo las premisas por soluciones interpretativas contradictorias e injustificable disparidad de trato, en relación a los muchas modalidades de comisión del crimen. A favor, AMORE et al., 2006: 100. CARINGELLA et al., 2011: 1052-1053. MONACO, 2011: 2334. CATULO, 930. D'AIETTI, 1994: 72. MUCCIARELLI, 1996: 99. PECORELLA, 2011: 5983. En contra, CADOPPI et al., 2011: 533.. PICA, 1999: 43.

[29] CUOMO y RAZZANTE, 2009: 99. BLAIOTTA, 2002: 2955. BLAIOTTA, 1999: 1642.

Descartada que la función de este elemento típico sea la expresión de la voluntad contraria del titular, lo que conduciría a defender sin titubeos la obligación de su previsión, la desvinculación de ambos componentes de la acción típica permite valorar en este momento la adecuación de su inclusión conforme a los principios generales del Derecho penal[30].

Del tenor literal del artículo 197.1 *bis* parece brotar la suposición de que, si el titular mantiene el sistema, ya sea de forma constante u ocasional, en comunicación con el exterior sin la disposición de medidas de seguridad, su comportamiento equivale a permitir el acceso a él de cualquier persona, tratándose de un acto impune y que no puede ser sancionado por la vía del Derecho penal[31]. Esta idea parece estar amparada en el carácter fragmentario de esta rama jurídica y en el principio de subsidiariedad, que constituyen los postulados básicos del principio de intervención mínima[32].

---

[30] En otra parte me he pronunciado acerca de la necesidad de subsistencia de este delito desde la perspectiva del principio de intervención mínima. Véase Introducción y Capítulo IV.

[31] Este elemento parece extraño hasta a la doctrina italiana. AMORE subraya al respecto que esta interpretación no se contradice con el hecho de que el artículo 615 *ter* del Código penal italiano permite también la incriminación de la conducta de permanencia no autorizada en el sistema informático protegido, en cuanto el legislador parece haber querido aludir a una conducta alternativa, poniendo como presupuesto de la permanencia abusiva la introducción lícita en el sistema protegido. AMORE et al., 2006: 106. PICA, 1999: 44.

[32] GONZALEZ RUS, 2005, II 1483. Por todos, MIR PUIG, 2005: 126-128 o Lección 4ª párrafos 47-49.

Sin embargo, la pregunta que cabe hacerse es si la utilización para cometer el delito de un procedimiento distinto a la superación las de medidas de seguridad no supone una afectación exactamente idéntica del bien jurídico protegido, ya sea éste la intimidad, la integridad del sistema o la seguridad informática[33]. En otras palabras, si el empleo de una mayor o menor intensidad o energía criminal por parte del sujeto activo modifica los parámetros de lesión del objeto al que el Derecho penal pretende ofrecer tutela conforme al principio de ofensividad[34].

[33] PICA compara esta idea con el domicilio tradicional, indicando que sería como no castigar a quien se introduce en el apartamento de otro, sin abrir la puerta principal pero pasando a través del buzón incorporado en la misma puerta por el mero hecho de que fuera de la puerta no hay escrito: prohibida la entrada. Es por ello que dicho autor afirma que si el domicilio informático es una extensión de la persona, y de su vida privada, o *rectius intima*, siempre debería ser protegido, y no sólo cuando el titular se haya precavido ante un acceso inconsentido disponiendo medidas de seguridad. Y, a tal efecto, considera que no es aceptable exigir que para poder tutelar el derecho de un sujeto sea necesario que este último haya demostrado, con la predisposición de medidas de protección, la voluntad de querer reservar el acceso al sistema informático, de modo que, en los casos de acceso es abusivo, incluso si carecen de medidas de seguridad adecuadas en el sistema del destinatario de la violación, el hecho es igualmente merecedor de sanción penal, al igual que sucede en el ámbito de la privacidad. A ello añade que con la previsión de las medidas de seguridad se dejan faltos de protección penal todo un conjunto de objetos personales a los que no se ha ofrecido protección por razones de coste o estructurales del sistema. PICA, 1999: 46-47.

En mi opinión, la respuesta a este interrogante es necesariamente afirmativa y ha de inclinarse a favor del bien jurídico en el sentido de entender que la reacción penal no es útil para cumplir su objetivo protector de un menoscabo de igual calibre pero substanciado por un procedimiento distinto[35]. Desde mi punto de vista debería, en consecuencia, castigarse también la conducta de quien accede al sistema en contra de la voluntad del titular sin vulnerar ninguna medida de seguridad[36].

En otro orden de cosas, desde la perspectiva de la prevención general se pretende con la incriminación positiva de este acto la coacción psicológica de la sociedad dirigida a evitar la comisión de todo tipo de accesos ilícitos al sistema informático, hecho que sólo se conseguirá ofreciendo una protección global a todos los ataques de la misma entidad sin discriminación alguna[37].

Establecida la nimia relevancia de este elemento en la configuración típica, resta examinar cuál es el efectivo papel que juega en el delito, sobre todo porque, como cabe recordar, el acceso ilícito constituye un tipo mixto alternativo integrado por dos conductas. Véanse, por tanto, como operan las restricciones aludidas en cada una de ellas.

---

[35] 1. La doctrina italiana también ha denunciado por lo que respecta a la inclusión de este elemento la existencia de una inminente ambigüedad en el artículo 615 ter del Código penal italiano de los demás tipos que se hallan en la ubicación sistemática donde se ha incriminado la conducta, los delitos contra el domicilio, en la medida en que considera que la limitación de la tutela penal únicamente vinculada a los sistemas protegidos con medidas de seguridad no se armoniza perfectamente con la idea de que la norma salvaguarde exclusivamente el domicilio informático, autorizando una reconstrucción en términos de ofensividad, en la cual resultaría tutelado también el bien de la *riservatezza* de los datos y programas. AMORE et al., 2006: 106.
2. Creo que de hecho esta idea es la que sustenta el hecho de que en el allanamiento de morada se castigue la entrada cuando la puerta está abierta.

[36] A favor, MUCCIARELLI, 1996: 99. PICA, 1999: 46. RELLA, 2007: 47. En contra, TRENTACAPILLI, 2002: 1283. MAIORANO, 2010: 1360.

[37] MIR PUIG, 2005: Lección 3ª párrafos 17-19..

3. APLICACIÓN A AMBAS MODALIDADES

Del tenor literal del artículo 197.1 *bis* parece desprenderse la aplicación de las dos cláusulas relativas a los medios comisivos a los dos comportamientos típicos previstos en el precepto. En efecto, el Código penal afirma *el que por cualquier procedimiento y vulnerando medidas de seguridad establecidas para impedirlo, acceda … o se mantenga*. Mientras que el inciso por cualquier medio o procedimiento no suscita, obviamente, conflicto interpretativo alguno, la vinculación de la previsión relativa a la vulneración de medidas de seguridad plantea problemas hasta tal punto que de *lege ferenda* incluso se propone su supresión[38].

Ciertamente, con la redacción de 2010, desde el punto de vista gramatical la redacción del tipo permite que la vulneración de las medidas se exija también en la modalidad de mero mantenimiento[39]. No obstante, si se afirma que la permanencia ilícita a los efectos típicos debe producirse con vulneración de las medidas de seguridad, ello significa:

> a) Por una parte, que en realidad lo que se está haciendo es acceder y no mantenerse, porque la superación de la medida es lo que marca el resultado de acceso, pero en el caso del

[38] SÁNCHEZ DOMINGO, 1998: 39.

[39] Así lo entienden también MORALES PRATS, 2011: 485. TOMÁS - VALIENTE LANUZA, 2010: 803. En cambio, otros autores como BERGHELLA-BLAIOTTA, consideran que el derribo de las defensas del sistema señala de desvalor de la acción, y que por lo tanto también en las hipótesis de permanencia abusiva tiene que manifestarse una conducta de serio contraste respecto a las defensas del sistema. BERGHELLA y BLAIOTTA, 1995: 2334. En igual sentido que los anteriores, PECORELLA, 2011: 5984.

mantenimiento la conducta es de mera actividad y posterior a ésta[40].

b) Por otra, si se ha accedido ilícitamente al sistema y, posteriormente, se permanece ilícitamente en él, este último comportamiento queda, según afirma la doctrina, absorbido por el acceso[41], o, más bien diría yo, (constituye un acto posterior impune o, si se quiere,) parte de la fase de agotamiento del delito.

En mi opinión, ambos motivos conducen no solo una restricción considerable del ámbito típico[42], sino a la directa inaplicación del artículo 197 *bis* del Código penal por lo que se refiere a la permanencia ilícita en un sistema informático. Así, la interpretación correcta según doctrina mayoritaria aduce que la vulneración de medidas de seguridad solo debe afectar al acceso pero no al mantenimiento, de modo que la finalidad de la norma es evitar que quien haya accedido al sistema con el consentimiento del titular permanezca en él tras su revocación al igual que sucede en el allanamiento de morada pasivo[43]. Se arguye también que esta alternativa hermenéutica, aunque amplia el ámbito de aplicación del precepto, tensiona la propia redacción típica del artículo 197[44].

---

[40] En Italia la Cass. Sez II 7 noviembre 2000 n. 1675 resuelve un caso de permanencia en el que se excluye la aplicación de las medidas de seguridad al considerarse que un propósito preciso de autorización del sujeto activo como la instalación de un programa o el mantenimiento del sistema no justifican la ulterior permanencia en el sistema. Según PECORELLA, la elusión de las medidas de seguridad no se tendrá en cuenta la hipótesis de permanencia en un sistema informático ajeno, contra la voluntad expresa o tácita del titular del *ius excludendi*, puesto que la introducción dentro del sistema habrá ocurrido legítimamente o de manera completamente casual. En este sentido, recoge el autor que excluyen la aplicación de la exigencia de infracción de medidas de seguridad. PECORELLA, 2011: 5984.

[41] SÁNCHEZ DOMINGO, 1998: 39.

[42] BOLEA BARDÓN, 2011: 468. MORALES PRATS, 2011: 485. TOMÁS - VALIENTE LANUZA, 2010: 803.

[43] MORALES PRATS, 2011: 485.

[44] BOLEA BARDÓN, 2011: 468. MORALES PRATS, 2011: 485. TOMÁS - VALIENTE LANUZA, 2010: 803.

La reforma operada en 2015 tiene visos de haber intentado solventar en cierto modo esta problemática, puesto que ha trasladado la referencia de a la voluntad en el acceso *sin la debida autorización* al inicio de la descripción típica. Esta modificación podría servir como base para defender la referencia de todos los elementos iniciales únicamente a la primera modalidad, pero creo que en realidad no hace más que aumentar el conflicto. Creo que la redacción perfecta de la norma pasaría por mover todos estos elementos al final de la conducta de acceso, tras la referencia al verbo y al objeto material.

Hasta que ello suceda, se tendrá que realizar una exégesis alternativa[45]. Para intentar salvar este escollo, propongo una interpretación propia (un tanto forzada, no voy a negarlo) pero que da plena viabilidad a la aplicación de la conducta de mantenimiento, posibilitando que la permanencia ilícita tras un previo acceso lícito pueda quedar subsumida en el artículo 197.1 *bis*. Mi propuesta personal se cimienta sobre tres ideas básicas que paso a detallar y que se estudiarán a lo largo de éste y otros capítulos:

a) La vulneración de las medidas de seguridad constituye un elemento típico totalmente diferenciado de la autorización.

b) La voluntad del titular opera como una causa de exclusión de la antijuridicidad no de la tipicidad.

3. La vulneración de medidas de seguridad supone la desactivación o superación de las mismas.

---

[45] Una perspectiva muy particular al respecto, coherente con la idea de exigencia de medidas de seguridad referida a las dos conductas es la que pone de relieve MUÑOZ CONDE. Este autor afirma que el tipo comprende tanto el acceso al sistema, como el mantenimiento dentro del mismo. La segunda modalidad es alternativa a la primera y supone que ha habido un acceso legítimo, pero que después, por as razones que sean, el titular del sistema cancela el permiso para ese acceso, lo que convierte la permanencia en ilegítima. Por tanto, concluye, si el sujeto sigue accediendo, se tratará de un acceso no autorizado, más que de un mantenimiento, aunque sea de preferible aplicación la modalidad de mantenimiento, ya que en realidad se trata de eso. No obstante, si la denegación del permiso va paralela a la adopción de medidas que impidan la continuación en el acceso (modificando, por ejemplo, la clave de acceso) la nueva entrada se debe incluir en el supuesto primero. MUÑOZ CONDE, 2010: 277-278.

4. VALORACIÓN PERSONAL

Pues bien, dicho lo anterior paso a explicar mi teoría. Si la vulneración equivale a desactivación o superación, y a su vez la desactivación o superación se encuentra desvinculada de la voluntad o autorización del titular, entonces la introducción de la contraseña correcta en el sistema supone también vulnerar las medidas de seguridad, siendo que la conducta es típica debiéndose valorar si está justificada o no. En este sentido, el acceso típico supondría la concurrencia de ambos elementos: vulneración de medidas de seguridad y ausencia de autorización del titular del sistema. Asimismo, si dicho titular revoca la autorización tras el acceso, puede afirmarse que ha existido vulneración de las medidas de seguridad puesto que éstas ya han sido desactivadas, siendo que ahora lo que tiene lugar es un mantenimiento ilícito porque se carece de la conformidad del propietario para permanecer en el sistema.

Esta tesis, que concede plena viabilidad a las pretensiones de la doctrina, tiene como resultado permitir la aplicación del artículo 197 *bis* manteniendo la vinculación de la vulneración a la segunda modalidad típica y, con ello, logrando la coherencia plena del tipo. Ello porque desligar, como propone la doctrina, ambos elementos tiene consecuencias de extrema trascendencia para el ámbito aplicativo del delito, situándolo en parte fuera del fin de protección de la norma.

Efectivamente, la supeditación de la vulneración de las medidas de seguridad solo a la conducta de acceso supondría ampliar desmesuradamente el ámbito aplicativo del precepto. Ello porque, si, como se ha dicho, la decisión del legislador es excluir de la tutela penal a los sistemas carentes de medidas de seguridad, en mi opinión, lo que se está consiguiendo con tal circunstancia es precisamente esto. Así pues, consecuencia necesaria de liberar a la conducta de mantenimiento del elemento vulneración de medidas de seguridad es la punición de los accesos producidos al sistema sin vulneración de las mismas, pero en este caso no por la vía del acceso

sino por la del mantenimiento ilícito. Me explico, si un sujeto ha accedido ilícitamente a un sistema que no dispone de mecanismos de protección, entonces su conducta es atípica conforme al acceso ilícito, pero perfectamente puede confirmar la tipicidad del mantenimiento ilícito, porque lo que se castiga es el acceso con vulneración de medidas de seguridad pero el mantenimiento sin vulneración de medidas de seguridad.

En consecuencia, la solución que propone la doctrina conduce, en realidad, a dar cabida a todos los supuestos de acceso ilícito a un sistema informático, tanto a los que suponen la vulneración de las medidas de seguridad como a los que no se han llevado a cabo a través de dicha vulneración, cuando se derive la conversión del acceso en mantenimiento ilícito, siendo que, desde mi punto de vista, entre ambos comportamientos existe una fina línea de separación.

Por tal motivo, para mí esta tesis acoge importantes peligros para los fines que en principio el Código penal pretende evitar, pues bajo la idea de dirigir solo la interpretación de las medidas de seguridad a la conducta de acceso, se está dando cobijo a los supuestos expresamente excluidos por decisión propia del legislador. Pues bien, delimitado el ámbito aplicativo del artículo 197 *bis*, pásese a estudiar su definición, naturaleza y tipología.

B) CONCEPTO, NATURALEZA Y TIPOLOGÍA DE MEDIDAS DE SEGURIDAD

1. CONCEPTO

La definición de qué debe entenderse por medidas de seguridad ha de empezar con una crítica. Así pues, antes de abordar la delimitación de este término, es necesario poner de relieve desde el punto de vista lingüístico la inadecuación de la terminología empleada para referirse al concepto de sistema protegido[46], ello por dos motivos:

a) Confusión terminológica: esta referencia ya posee funcional y nominalmente otro sentido en esta rama del Derecho[47], hecho que dificulta su interacción sistemática dentro del ordenamiento jurídico-penal en su conjunto[48]. Efectivamente, el concepto de medidas de seguridad tiene en nuestro sistema jurídico un significado muy concreto, vinculado a la peligrosidad criminal del sujeto, teniendo unos principios y presupuestos materiales propios[49].

b) Dificultad para delimitar su alcance: dentro del amplio espectro que pueden integrar las medidas de seguridad en el ámbito informático, resulta complicado determinar exactamente cuáles son aquellas que el Derecho penal debe tener en cuenta[50]. Ilustradora resulta en el ámbito español la utilización del inciso *establecidas para impedirlo*, el cual permite identificar con mayor certeza las funciones que deben tener éstas, actuando como linde de la protección penal. A él me referiré más tarde.

---

[46] CADOPPI et al., 2011: 532. CANNATA, 2006: 534. GALDIERI, 1997: 154. PICA, 1999: 52.

[47] CADOPPI et al., 2011: 532.. PICA, 1999: 52..

[48] GALDIERI, 1997: 154..

[49] MIR PUIG, 2005: 761 o Lección 34 párrafo 10 y ss..

[50] A favor, GALDIERI, 1997: 154.. En contra, CANNATA, 2006: 534..

Entiendo que fórmulas más idóneas para describir las distintas vías a través de las cuales se articula la protección del sistema frente al acceso ilícito por parte de terceros serían las de sistema informático protegido o sistema dotado de medios de protección específicos[51]. La mayor corrección de estas propuestas en su mayor concreción, en primer lugar porque toman como referencia el sistema informático (objeto sobre el que tienen que estar dispuestas las medidas) y, en segundo lugar, porque permiten ver la idea de exclusividad (idoneidad) que éstas tienen que tener, características ambas a la que se hará referencia en los próximos apartados.

No obstante, el uso de la expresión medidas de seguridad está muy arraigado a todos los niveles: nacional, internacional, comunitario y comparado. En efecto, se trata de un término de uso totalmente corriente en los estudios y documentos nacionales y supranacionales sobre Derecho informático, sin olvidar que constituye la traducción de un vocablo de origen anglosajón, siendo el inglés el idioma vehicular en el que se expresa (y que domina) el lenguaje informático[52].

2. Pues bien, explicada mi opinión en relación con la denominación que se ha atribuido a este elemento del tipo, paso a ocuparme de la efectiva definición del concepto medidas de seguridad. A tal efecto, el Código penal español, al igual que sucede en la inmensa mayoría de países, no nos dice qué debemos entender como tales. En mi opinión, en la medida en que la descripción típica no ha previsto ningún elemento definidor o de restricción que deba tomarse en consideración al margen del inciso *establecidas para impedirlo*, éstas deben quedar conceptualizadas desde la perspectiva más amplia, actuando como único criterio rector el bien jurídico protegido en el delito (interpretación teleológica).

---

[51] Curiosamente, aunque en la doctrina italiana se han realizado fuertes críticas a esta expresión, ningún autor ha propuesto un término alternativo para sustituirlo. Este es el término adoptado en ALEMANIA. Véase Capítulo II.

[52] Igualmente, CADOPPI et al., 2011: 534. GALDIERI, 1997: 154. PICA, 1999: 52.

En general, la concreción de este elemento se lleva a cabo por la doctrina partiendo desde una doble perspectiva: por una parte, atendiendo al objeto, es decir, al elemento físico en el que se materializan las medidas de seguridad, y, por otra parte, atendiendo a la finalidad que estas deben satisfacer, esto es, el propósito con el que han sido establecidas. Me parece adecuado aunar ambas ideas para adoptar una noción común.

Aunando ambas posturas[53], creo oportuno definir medidas de seguridad como todo dispositivo, medio, instrumento o mecanismo de protección del sistema, que tiene por finalidad la selección de los sujetos habilitados para acceder al sistema informático, excluyendo a

---

[53] Tomando como punto de referencia el objeto, BORRUSO constriñe la definición al significado descriptivo de los medios de protección puramente informáticos, mientras que PECORELLA las amplia a cualquier elemento a cuya superación es posible subordinar el acceso a datos y a programas contenidos en el sistema. Por el contrario, defienden la noción finalística PICA, MARINI y MANTOVANI, que recogen una definición casi idéntica. PICA señala que debe entenderse como tales cualquier impedimento dispuesto en esencia para impedir el acceso al sistema informático por parte de personas no autorizadas, en el mismo sentido de MANTOVANI, quien afirma que son los dispositivos idóneos para impedir el acceso al sistema a los sujetos no autorizados, MARINI según afirma la doctrina mayoritaria, cualquier instrumento, mecánico o electrónico, capaz de efectuar una distinción de los sujetos autorizados a acceder al sistema informático o telemático. A todo ello aclara FIANDANCA que se trata de cualquier mecanismo de selección de los sujetos habilitados para el acceso al sistema protegido. En una posición mixta y no muy afortunada, CECCACCI las define como aquel conjunto de características técnicas en software y hardware actúa para impedir la entrada de terceros a los archivos (información y datos) y programas contenidos y se almacena de forma confidencial en los sistemas informáticos y de telecomunicaciones. Más acertado está CUOMO al interpretar como tales cualquier herramienta, aplicación o dispositivo encargado de asegurar el acceso a un sistema informático o, más bien, formuladas en sentido negativo, cualquier tipo de protección que suponga la selección de los sujetos habilitados para el acceso al sistema. Todas estas definiciones tienen su origen en la Sentencia de 7 de noviembre del 2000, nº 12732, CP, 2002, pág. 249, y a la que posteriormente han seguido muchas más como Cass. Senz. II, 4 maggio 2006, n. 30663, Dir. pen e proc. 2007, 363. Dicha resolución afirma que adquiere relevancia cualquier mecanismo de selección de los sujetos habilitados para el acceso al sistema informático, aunque cuando se trate de instrumentos externos al sistema y meramente organizativos, en cuanto destinados a regular el acceso mismo al local en el cual son custodiados. Esta definición es la que acoge literalmente un importante sector de la doctrina como CADOPPI o CANNATA. BORRUSO et al., 1994: 29. CADOPPI et al., 2011: 532. CANNATA, 2006: 534. CECCACCI, 1994: 71. CUOMO y RAZZANTE, 2009: 100. PECORELLA, 2011: 5984. FIANDANCA y MUSCO, 2013: 294. MANTOVANI, 2011: 545. MARANI, 2007: 617. PICA, 1999: 53.

terceros ajenos al mismo[54] y también procurando la reserva del contenido[55].

La noción propuesta se integra, por tanto, por un elemento de carácter positivo, el material, en el sentido de que el número de mecanismos de protección a utilizar debe contemplarse en su más amplia extensión, debiendo entenderse englobados cualquiera de los ya existentes pero también los que pudieran surgir como consecuencia de la innovación tecnológica; y otro de carácter negativo, basado en la restricción que conlleva la limitación de la función de las mismas en cuanto a que su destino sea salvaguardar el sistema de intrusiones externas, reservando su contenido solo al titular o a quien éste autorice.

---

[54] A favor, AMORE et al., 2006: 100. CARINGELLA et al., 2010: 1052-1053. CRESPI et al., 2011: 2334. CATULO, 930.D'AIETTI, 1994: 72. , PECORELLA, 2011: 5983. FIANDANCA y MUSCO, 2013: 294. MUCCIARELLI, 1996: 99. PICOTTI, Studi di Diritto penale, 114.

[55] Cierto sector de la doctrina italiana considera que el bien jurídico protegido es la riservatezza de los datos y programas contenidos en el sistema informático, motivo por el cual defienden que la función principal de esta previsión no es otra que la de procurar la reserva de éstos. En este sentido, entiende PECORELLA que solo el titular que demuestra interés y responsabilidad adoptando los medios idóneos para impedir el acceso puede beneficiarse de la tutela penal. Esta es a mi juicio la opción a la que se adhiere la *Relazione di presentazione dello Schema di Progetto di legge contenente modificazioni ed integrazioni delle norme del Codice penale in tema di criminalità informática*, que justifica la limitación de los sistemas informáticos o telemáticos a aquellos únicamente protegidos por medidas de seguridad en el hecho de que, debiéndose tutelar el derecho de un específico sujeto, es necesario que este último haya demostrado, con la predisposición de medios de protección lógicos o físicos (materiales o personales) la voluntad expresa de reservar el acceso y la permanencia en el sistema a las personas autorizadas. PECORELLA, 2011: 5983. A favor ALMA y PERRONI, 1997: 505. BORRUSO et al., 1994: 28. CERQUA, 2000: 53. CUOMO y IZZI, 2002: 1021. MANTOVANI, 2011: 518-521. TRENTACAPILLI, 2002: 1283. Relazione di presentazione dello Schema di Progetto di legge contenente modificazioni ed integrazioni delle norme del Codice penale in tema di criminalità informática, Documenti Giustizia, 1991, n. 9, 142 y ss.

La conjunción de estos dos factores, sin soslayar ninguno de ellos, es lo que, a mi juicio, permite establecer una acotación perfecta de qué debe entenderse por medida de seguridad, el primero, porque elimina toda discusión con respecto a los posibles medios y, el segundo, porque permite seleccionar de entre todas las medidas de seguridad existentes las que quedan englobadas en el tipo penal, tal y como, de hecho, dispone el propio artículo 197 *bis* del Código penal al añadir la coletilla *establecidas para impedirlo*[56].

En consecuencia, este concepto concuerda perfectamente con las apreciaciones que más tarde realizaré al analizar las distintas cuestiones con profundidad[57]. Sirva ahora la sintetización de las mismas en una frase como medio para avanzar al lector cuál va a ser mi posición: desde un punto de vista negativo, solo deben considerarse medidas de seguridad aquellas que verdaderamente están destinadas de forma directa y exclusiva a evitar el acceso al sistema informático (criterio de la idoneidad)[58], pero desde una perspectiva positiva, lo anterior debe tener lugar con independencia de que dichos medios tengan una naturaleza material (medidas de seguridad física)[59] o inmaterial (medidas de seguridad lógica)[60].

Aclarado, pues, el concepto de medidas de seguridad, me parece oportuno empezar a abordar cada uno de los aspectos del mismo, es decir, la tipología y la naturaleza de éstas. Aunque lo lógico sería empezar por la naturaleza de las mismas, para una mayor comprensión de ésta se hará referencia en primer lugar a los tipos de medidas.

---

[56] Véase Apartado III. de este Capítulo.

[57] Véase Apartado III de este Capítulo.

[58] BORRUSO et al., 1994: 29. MANTOVANI, 2011: 545. MARANI, 2007: 617. PICA, 1999: 53.

[59] Véase próximo apartado.

[60] Véase próximo apartado.

3. TIPOLOGÍA

Determinadas cuáles son las medidas de seguridad que podemos hallar vinculadas al sistema informático, se plantea como necesario, a continuación, ofrecer una definición de sendos subgéneros de medidas. La delimitación de este aspecto permitirá, luego, esbozar un esquema material de las distintas posibilidades existentes. Conózcase pero, primero, la noción de cada una de ellas:

> **a) Medios de carácter lógico:** éstos vendrían a integrarse por aplicaciones de tipo software, esto es, conjuntos de impulsos electrónicos, por lo general en forma de combinaciones de letras y/o números, almacenados en el sistema y conocidos sólo por aquellos que están autorizados a acceder al sistema y que deben ser comunicar a ésta la combinación correcta para hacer viable su acceso[61].
>
> **b) Medios de carácter físico:** dentro de ellos cabe distinguir:
>
> > **b.1) <u>Instrumentos hardware</u>:** son medios físicos de clausura y aislamiento del sistema informático[62] integrados en su estructura material y que posibilitan su funcionamiento tras su desactivación[63].
> >
> > **b.2) <u>Mecanismos de tipo organizativo</u>:** se trata de aquellos mecanismos externos de carácter personal o material cuya finalidad es, o bien la custodia directa del sistema informático, o bien la restricción del acceso al lugar donde éste se encuentra[64].

Para describir desde una perspectiva técnico-material las medidas de seguridad expuestas[65], obsérvese de forma pormenorizada en qué puede consistir cada una de ellas:

---

[61] PICA, 1999: 53..

[62] CANNATA, 2006: 535.. CADOPPI et al., 2011: 534.. PECORELLA, 2006: 325.. PICA, 1999: 54..

[63] PICA, 1999: 54..

[64] CUOMO y RAZZANTE, 2009: 101..

[65] Algunos autores han intentado sintetizar las distintas medidas de seguridad en una categorización propia basándose en criterios puramente dogmáticos. Así, por ejemplo, CORRERA y MARTUCCI, 1986: 46-47..

a) MEDIDAS DE SEGURIDAD FÍSICA

ii) INSTRUMENTOS HARDWARE: MEDIOS DISPUESTOS DIRECTAMENTE SOBRE EL OBJETO

1. Llave metálica de acceso al propio sistema: consiste en un tipo de llave cuya conexión al sistema permite conseguir la realización de cualquier tipo de *input*[66].

2. Badge o tarjeta magnética de plástico o material similar: que incorpora cierto usuario con capacidad de datos de descubrimiento para el acceso y para ser utilizado en la forma de la llave, usualmente introduciendo la banda magnética en un lector de tarjetas[67], de manera que permite efectuar el proceso de autenticación o de identificación del usuario habilitado al acceso[68].

3. Criptografía: **Chip TPM (Trusted Platform Module).**

ii) INSTRUMENTOS DE TIPO ORGANIZATIVO (ESTABLECIDOS PARA CUSTODIAR EL SISTEMA)

Especial controversia suscita en la doctrina italiana la reconducibilidad a tal categoría de medidas de seguridad las protecciones dispuestas no directamente sobre el sistema informático, sino para impedir el acceso al lugar donde éste se encuentra custodiado.

1. Puerta blindada.

2. Personal de vigilancia: Cass Sez. V 8.7.2008, 7, 11, 2000

---

[66] BORRUSO et al., 1994: 30.. CADOPPI et al., 2011: 534.. CANNATA, 2006: 535.. PECORELLA, 2006: 325..

[67] Algunos autores como CADOPPI se refieren a ellas como una medida de carácter lógico y no físico. CADOPPI et al., 2011: 534..

[68] CANNATA, 2006: 535.. CUOMO y RAZZANTE, 2009: 99.. PAPA los incluye como subtipo de medidas de carácter lógico, al entender que se trata de un código memorizado en la banda magnética de la tarjeta.

b) MEDIDAS DE SEGURIDAD LÓGICA

Existen un número importante de sistemas técnicos de control destinados a crear barreras electrónicas, diseñadas para bloquear y reportar cualquier intento de acceso, sin autorización, en la memoria de los programas o datos[69]. Además, en los sistemas de elevada complejidad, están presentes varios planos de interdicción de área y de función (dominio), cada uno de los cuales dispone de sus propias medidas de seguridad[70]. Por tal motivo, voy a reseñar únicamente los más corrientes:

> **1. *Password* o llave lógica**: consisten en una palabra (logos) o más palabras o por número o por una combinación de caracteres alfanuméricos (compilable y modificable como y cuando quiere programador ad libitum y, en los programas más sofisticados, del mismo usuario) con función de ábrete sésamo, que siendo tecleada en el ordenador de forma exacta permite al usuario acceder al concreto sistema o al contenido de éste[71]. En este sentido, afirma BORRUSO que salvo que no sean digitadas exactamente, y, a veces, en la secuencia debida o con el respeto de determinados intervalos de tiempo, no se logra enlazarse con el ordenador o bien a penetrar en los archivos[72]. La jurisprudencia y doctrina italiana consideran como tal la contraseña originalmente instalada por el proveedor del sistema que el cliente nunca a reemplazado[73]. Dentro de esta posibilidad, se puede fortalecer las medidas de protección mediante[74]:

---

[69] CORRERA y MARTUCCI, 1986: 47..

[70] CUOMO y RAZZANTE, 2009: 99..

[71]CUOMO y RAZZANTE, 2009: 99.. CRESPI et al., 2011: 2334.. DOLCINI y MARINUCCI, 2011: 5984.. Cass Pen 21.2.2008 Sez. II 08/3671

[72] BORRUSO et al., 1994: 30..

[73] Cass. Pen. 7-11-2000, n. 12732, in Cass. Pen 2002, 249; nota de FLOR, 111. CADOPPI et al., 2011: 534..

[74] CORRERA y MARTUCCI, 1986: 47..

a) <u>Código individual:</u> en este caso un único usuario conoce la contraseña, sin que la combinación de la que ésta consta sea revelada por esta persona a nadie más[75].

b) <u>Código de grupo</u>: cuando el trabajo es en grupo

2. <u>Programas o aplicaciones dirigidos a proteger el sistema</u>[76]: afirma CORRERA que a otro nivel, se pueden desarrollar programas para empresas comerciales que reportan como los datos para la entrada y la actividad de la desviación del ordenador de una serie de funciones que anteriormente supone que es aceptable, o que, mediando mecanismo de revisión especial, son capaces de evitar que esto suceda[77]. Dentro de éstos, cabe destacar las **<u>extensiones de seguridad del navegador</u>** con la finalidad de impedir el acceso o la propagación de virus[78].

Para algunos autores resultan asimilables a las medidas de seguridad otro tipo de protecciones de los datos como:

3. <u>Sistemas biométricos con datos antropométricos</u>[79]: supone la memorización por parte del sistema de alguna característica física irrepetible del usuario habilitado al acceso, que viene a ser memorizada en el ordenador y es confrontada con aquella de la persona que intenta utilizar el recurso informático[80], por ejemplo huellas dactilares, geometría de la mano, timbre de la voz, retícula venosa de la retina ocular y otros destinados a ser

---

[75] Admite la contraseña como medida de seguridad válida en aplicación del artículo 197.3 la Sentencia de la Audiencia Provincial de Girona (Sección 4ª) número 358 de 22 de junio de 2015.

[76] CADOPPI et al., 2011: 534..

[77] CORRERA y MARTUCCI, 1986: 48..

[78] Tribunal de Bologna 22.12.2005, CG, CM, 2006, 759.

[79] La doctrina afirma que se trata de medidas que deben ser asimilables a las anteriores.

[80] CUOMO y RAZZANTE, 2009: 99..

detectados por sensores. Se trata de las técnicas más avanzadas y modernas utilizadas para sistemas de alto riesgo como por ejemplo bases militares o de alta tecnología[81].

4. Criptografía: la codificación criptográfica secreta es, según la doctrina, el método más eficaz para la evitar el acceso al sistema informático. Se trata de una técnica capaz de codificar o encriptar la información mediante el uso de claves secretas. En este contexto, desde 1977, existe el Data Encryption Standard Model, que se basa en una llave electrónica formada por un máximo de 56 bytes (elementos) y le permite hacer que los datos sean ilegibles para cualquier persona que no la posea.

[81] ALEO y PICA, 2012: 55..

3. NATURALEZA

Desde un punto de vista técnico-formal, resulta sumamente fácil identificar específicamente la tipología y naturaleza exactas de los posibles medios de protección que pueden disponerse sobre los sistemas informáticos[82]. No obstante, en el ámbito jurídico esta delimitación resulta bastante más compleja, pues deberá analizarse en cada caso la adecuación de éstos a la definición propuesta, ya que el legislador no ha precisado la calidad, la naturaleza o la eficacia que deben tener, limitándose a prever, como se ha indicado, solo la necesidad de su presencia[83].

El siguiente paso, por consiguiente, supone precisar cuáles son los dispositivos o instrumentos específicos destinados a impedir el acceso al sistema, ello siempre debiendo tenerse en cuenta que ningún sistema de seguridad podrá garantizar una seguridad absoluta, a causa de la variedad de riesgos presentes en la actual sociedad del riesgo y de la previsible y siempre creciente agresividad y preparación del criminal informático[84].

Ofreciendo una respuesta a dicha cuestión, cabe decir que la naturaleza de tales medidas de seguridad puede ser únicamente de dos tipos: físicas o materiales o lógicas o inmateriales[85]. Dentro de estos dos subgéneros de medidas de protección a disponer sobre el sistema informático, no existe a día de hoy un acuerdo unánime en la doctrina comparada acerca de cuáles deben ser los admitidos.

---

[82] CADOPPI et al., 2011: 532..

[83] CADOPPI et al., 2011: 534..

[84] CORRERA y MARTUCCI, 1986: 49.

[85] Algunos autores como PICA o CECACCI denominan a las medidas de seguridad de tipo físico, medidas de hardware, y a las de carácter lógico, medidas tipo software. A mi modo de ver, esta distinción no es adecuada porque, como se verá, dentro de los mecanismos de protección de carácter físico también se incluyen medios organizativos de carácter personal o instrumentos que no pueden ser considerados como hardware. Por esta razón rechazo esta clasificación inclinándome a favor de la usada en el presente estudio. CECCACCI, 1994: 71. PICA, 1999: 54.

En general, la inclusión de las medidas de tipo lógico en el elemento objetivo del tipo es una cuestión más pacífica aunque no exenta de conflicto, suscitándose el debate principal en torno a la subsunción de las medidas de tipo físico. En este sentido, el punto de discusión más crucial se centra no ya en si deben admitirse o no, sino, en caso de ofrecer una respuesta afirmativa, en cuáles de ellas deben de ser las efectivamente tenidas en cuenta. Se presenta con detalle la problemática surgida en torno a esta temática.

a) DISCUSIÓN SOBRE LAS MEDIDAS DE TIPO LÓGICO

Un sector muy minoritario de la doctrina penal, en una interpretación excesivamente restrictiva del tipo, excluye de la noción jurídica de medidas de seguridad no solo los medios de carácter físico, sino también ciertos instrumentos de protección de carácter lógico que, sin embargo, sí quedarían englobados en dicho concepto desde un punto de vista técnico. Adopta como fundamento la exigencia de cierta complejidad técnica en el sistema de protección[86], el género plural usado en la Ley[87] o, incluso, la captación externa y no simbólica de la voluntad expresa de exclusión[88]. Afortunadamente, esta tesis ha sido rebatida sobre la base de la compatibilidad de este tipo de medidas con el tenor de la ley, de que la utilización del plural sólo representa un enlace gramatical en paralelo con los sistemas y de que la predisposición de una protección fácilmente superable no excluye la subsistencia del delito[89].

---

[86] En general, se negaba la eficacia de las claves o códigos de acceso considerar que ésta es nula, las cuales eran calificadas por CORRERA como *el más grande engaño de la seguridad del sistema informático*. Las razones de tal alegato: *no se cambian tan habitualmente como se debiera, no se modifican aquellas que vienen predispuestas por el fabricante e, incluso, en multitud de ocasiones se transcriben en agendas o diarios o en algún lugar del mismo sistema*. Sobre CORRERA y MARTUCCI, 1986: 49.

[87] CECCACCI, 1994: 70 y ss.

[88] A ello añade BERGHELLA-BLAIOTTA afirman que las medidas de seguridad deben ser un hecho, un obstáculo tan serio como difícil de remover; solo así se estará evitando el riesgo de una criminalización indiscriminada. BERGHELLA y BLAIOTTA, 1995: 2334.

[89] CUOMO y RAZZANTE, 2009: 101. Véase Apartado III. de este Capítulo.

b) DISCUSIÓN SOBRE LAS MEDIDAS DE TIPO FÍSICO

Entre los autores que admiten la inclusión de las medidas de seguridad de tipo físico pueden distinguirse dos corrientes: una que entiende que deben solo quedar englobados los mecanismos instalados directamente sobre el sistema y otra que, junto a ellos, incorpora también los elementos dispuestos para proteger la entrada al lugar donde éste se encuentra, a la que yo me adhiero y de la que se desprende ineludiblemente el examen de la relación entre este delito y el de allanamiento de morada. Asimismo, todos ellos dan por sentado la subsunción en el tipo de las medidas de tipo lógico.

1. Posición intermedia: en un punto intermedio entre la posición más restrictiva, ya apuntada, y la más abierta, que se expondrá más tarde, se halla la tesis de aquellos autores que se pronuncian a favor de la inclusión de los medios de protección lógicos del sistema y también de aquellas medidas físicas estrictamente dirigidas a la tutela del *hardware* o del *software* del sistema[90]. En efecto, para ellos no cabe vincular la interpretación de este elemento objetivo a la interdicción de los mecanismos que hubieran podido disponerse para impedir el acceso al lugar en el que está situado el sistema con base en tres argumentos:

---

[90] Un tanto contradictorio resulta CUOMO en este punto, pues tras definir las medidas de seguridad como aquellos mecanismos lógicos, tecnológicos y organizativos que tienden a impedir la comisión de delitos informáticos y a prevenir otros eventos dañosos para la máquina o para los datos, a continuación, sin embargo, puntualiza que más que los medios de protección del lugar donde se encuentra el equipo, se trata de herramientas de protección que implican directamente y exclusivamente el sistema informático. En consecuencia, dicho autor, se estaría en realidad adhiriendo a esta segunda tesis. BORRUSO et al., 1994: 29. CADOPPI et al., 2011: 535. CANNATA, 2006: 535-536. CARINGELLA et al., 2010: 1053. CUOMO y RAZZANTE, 2009: 100. FONDAROLI, 1996: 291 y ss. GALDIERI, 1997: 154. MAIORANO, 2010: 1360. MANTOVANI, 2011: 521 y 545. PECORELLA, 2011: 5985. PLANTAMURA y MANNA, 2007: 45-46. En España, sin especificar demasiado aunque solo mencionando a título de ejemplo como medidas de seguridad las impuestas directamente sobre el sistema, GONZÁLEZ RUS, 2011: 521.

a) Idoneidad[91]**:** Este tipo de medidas no son idóneas al fin pretendido por la norma puesto que integran tan solo una protección indirecta y eventual del sistema informático. Lo primero, porque el propósito principal y directo de la predisposición de las medidas de tutela del lugar es prevenir el riesgo de daños de los componentes físicos o lógicos del sistema. Lo segundo, porque el mismo instrumento no puede relacionarse con el acceso abusivo cometido de forma remota, en el que el autor se vale del auxilio de un instrumento informático o telemático. Debo rechazar esta idea porque resulta aplicable no solo a este tipo de medidas, sino a todos los mecanismos de protección que pudieran instalarse en el sistema: por una parte, el cierre del lugar tiene más finalidades que la de evitar daños en los componentes físicos, desde el hurto del sistema hasta prevenir el acceso ilícito; por otra, incluso en el acceso remoto pueden ser numerosas las variantes de medidas de seguridad vulneradas, pero no todas ellas se verán afectadas por el acceso, puede que únicamente se produzca la superación de una sola o de varias de ellas.

b) Interpretación extensiva[92]**:** La descripción típica no efectúa ninguna mención al respecto y si hubiera sido la voluntad del legislador la inclusión de tales elementos hubiera dotado de mayor concreción a la expresión medidas de seguridad, redimensionando el ámbito de aplicación del delito. Se considera a este respecto que englobar los instrumentos externos o organizativos del sistema supone realizar una

[91] CADOPPI et al., 2011: 535.. FONDAROLI, 1996: 291 y ss..

[92] PLANTAMURA y MANNA, 2007: 45-46..

interpretación extensiva del tipo prohibida en Derecho penal. Este razonamiento tampoco puede ser compartido, puesto que lo que indica el silencio del legislador es precisamente lo contrario: *ubi lex non distinguit, nec nos distinguere debemus*. Toda interpretación se mueve dentro del límite del sentido literal de la ley, incluso la extensiva, la cual resulta admisible en Derecho penal siempre que no sobrepase el límite de garantía representado por la letra de la Ley[93]. Fuera de estos márgenes, que no es el caso, nos hallaríamos ya en el campo de la analogía, cuya aplicación *in malam partem* sí que es rechazada por el Derecho penal[94].

c) Objeto: No puede concebirse una medida de seguridad sino es en conexión material con el sistema, pues éste es el objeto del delito y, por tanto, sobre él se proyecta el bien jurídico[95]. Este tercer argumento también debe ser descartado ya que el bien jurídico servirá como guía para valorar si la medida se ajusta al fin pretendido, pero no es posible ofrecer un criterio apriorístico, sino que deberá valorarse en cada caso concreto.

2. Postura abierta: Por último, la opinión más amplia de todas arguye a favor de encuadrar en el texto legal todo el abanico de medidas expuesto, esto es, tanto las de carácter lógico como las de tipo físico y, dentro de éstas, las directamente

[93] MIR PUIG, 2005: 124-125 o Lección 4 párrafo 42.

[94] MIR PUIG, 2005: 124-125 o Lección 4 párrafo 42.

[95] PECORELLA, 2011: 5985. MANTOVANI, 2011: 545.

establecidas sobre el sistema y las dirigidas a proteger la entrada al lugar donde éste se encuentra[96].

a) Los defensores de esta tesis poseen en Italia un eslabón legal muy poderoso, pues el apartado 2 del artículo 615 *ter* del Código penal italiano castiga con mayor pena la comisión del hecho cuando el autor use violencia sobre las personas, fuerza en las cosas, o cuando porte armas[97]. En este sentido, manifiesta la doctrina italiana que tales agravantes solo pueden concurrir en caso de presencia física del sujeto que realiza la acción en el lugar donde se encuentra el sistema informático y respecto a elementos físicos[98].

---

[96] Esta tesis ha sido respaldada, asimismo, por la jurisprudencia italiana mayoritaria, que ha acogido una noción extremadamente amplia de medidas de seguridad, asumiendo la relevancia de cualquier mecanismo de selección de los sujetos habilitados al acceso, aunque se trate de instrumentos externos al sistema o meramente organizativos destinados únicamente a regular el acceso al lugar donde se encuentra el sistema informático. La apertura de ésta es tal que resta importancia al hecho de que el titular no haya adoptado las medidas mínimas de seguridad exigidas por la Ley, caso en el que hace prevalecer la ausencia de consentimiento sobre la efectiva funcionalidad operativa o sobre la real eficacia protectiva o disuasoria de las medidas de seguridad. CUOMO y RAZZANTE, 2009: 101. A favor, en España, MORALES PRATS, 2011: 484. En Italia ALIBRANDI, 2011: 1758. CRESPI et al., 2011: 2334. CADOPPI et al., 2011: 534. CANNATA, 2006: 535-536. DELPINO, 2003: 585, DESTITO et al., 2007: 84. DI GIANNANTONIO, 2001:. FIANDANCA y MUSCO, 2013: 294. GALDIERI, 1997: 154, MARANI, 2007: 617. PALAZZO y PALIERO, 2011: 300. PICA, 1999: 52. PECORELLA, 2006: 326. PICOTTI, 2004: 22.

[97] *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: ... 2) se il colpevole per commettere il fatto usa violenza sulle cose o alle persone, ovvero se è palesamente armato.

[98] PECORELLA, 2011: 5984. GALDIERI, 1997: 154. PICA, 1999: 52. PICOTTI, 2004: 22.

b) En adición a los argumentos ya expuestos para rebatir la posición anterior, esto es, la tesis intermedia, la restricción de las medidas de seguridad no aparece confirmada por el tenor de la ley -o, en tal caso, éste es absolutamente insatisfactorio[99]- puesto que la amplia redacción que el legislador ha ofrecido a la conducta típica parece legítimamente susceptible de la más amplia interpretación[100].

c) Además, teniendo en cuenta que he señalado que el único criterio que se desprende del tenor legal es que las medidas tengan una función de exclusión de terceros y reserva del contenido, o sea, que hayan sido *establecidas para impedir* el acceso, considero oportuno defender que, para cumplir tal cometido, es suficiente con cualquier instrumento de protección[101].

---

[99] PICA, 1999: 52..

[100] PICA, 1999: 53..

[101] DESTITO et al., 2007: 84.. FIANDANCA y MUSCO, 2013: 294.. GALDIERI, 1997: 155.. MARINI, 617.

4. CUESTIONES CONCURSALES

Admitir que las medidas de seguridad pueden ser violadas también de forma física mediante el acceso al lugar donde se encuentra el sistema informático tiene como corolario penetrar en cierta medida en los difusos contornos del ámbito típico del delito de allanamiento de morada y del delito de daños.

a) DELITO DE ALLANAMIENTO DE MORADA

El allanamiento de morada se configura en nuestro Código penal como una figura puente para muchos otros delitos. La razón para tal afirmación estriba, por una parte, en que es un delito de mera actividad, que no requiere más que de una acción en sentido estricto en el caso de la entrada (allanamiento activo) y de una omisión propia en el caso del mantenimiento (allanamiento pasivo), motivo por el cual los distintos resultados producidos se considerarán infracciones diferenciadas de éste; y, por otra, en que se trata de un delito permanente, en el que la consumación se prolonga tanto como perdure la constricción del derecho, lo que supone una coincidencia temporal lógica entre éste y el otro delito[102]. Esta especial naturaleza del delito plantea innumerables dificultades a la hora de determinar sus relaciones con las demás infracciones penales con las que pueda concurrir[103], aunque en el delito de acceso ilícito, la específica ubicación sistemática de este último limita inapropiadamente el número de conflictos posibles[104].

---

[102] Concretamente, SANZ MORÁN entiende que se trata de un delito eventualmente permanente, lo que significa que el hecho previsto en la ley puede agotarse en el momento en el que se concretan sus elementos constitutivos, pero también puede prolongarse. En otras palabras, basta con la realización de la conducta típica para su consumación, pero la continuación de dicha conducta no multiplica el número de delitos. SANZ MORÁN, 1986: 116. SANZ MORÁN, 2006: 37. SUÁREZ MONTES, 1968: 889.

[103] SANZ MORÁN, 2006: 83.

[104] Cabe tener en cuenta que el ámbito aplicativo del allanamiento de morada cada vez es más extensivo, pues se reconoce el derecho a la inviolabilidad del domicilio a distintos lugares anteriormente de dudosa aplicación. Así hay que tener en cuenta que la reciente jurisprudencia ha entendido subsumible en el delito de allanamiento de morada no solo los domicilios de los estudios profesionales, sino también los de los establecimientos industriales. Tales pronunciamientos constituyen hoy en día en nuestro y en otros países de nuestro entorno jurisprudencia consolidada. GALDIERI, 1997: 154.. ESPAÑA

Así pues, teniendo en cuenta que el artículo 197 *bis* se encuentra regulado entre los delitos contra la intimidad, tan sólo es posible afirmar la colisión entre éste y el allanamiento de morada de persona física del artículo 202 del Código penal, debiendo quedar excluidos el allanamiento de persona jurídica o el de establecimiento abierto al público del artículo 203 del Código penal. No obstante, la correcta fijación del bien jurídico fuera del ámbito de la intimidad supondría la modificación de este aspecto, pudiendo también plantearse conflictos con este segundo tipo penal relativo a la inviolabilidad del domicilio.

A los efectos de proporcionar una solución favorable a los conflictos derivados del allanamiento de morada con otros delitos, la Fiscalía General del Estado resolvió que *todos los casos en que la entrada o permanencia ilícita en la morada ajena conviva con otra infracción penal se penarán a través de las normas del concurso de delitos que muchas veces será medial (artículo 77), aunque no es descartable que, en ocasiones, haya que acudir al sistema ordinario de punición del artículo 73 por tratarse de un concurso real puro*[105]. Esta idea es aceptable teniendo en cuenta

---

[105] Como muy bien pone de relieve SANZ MORÁN, no resulta claro el criterio con arreglo al cual resuelve el Tribunal Supremo este tipo de situaciones, sobre todo teniendo en cuenta que se trata de un delito permanente. Dicho autor, de una forma absolutamente acertada, plantea la cuestión de la siguiente forma: Existirá un concurso ideal de delitos entre el allanamiento de morada y los delitos cometidos para la perpetración o el mantenimiento de la situación antijurídica. Habrá, por el contrario, un concurso real entre el allanamiento de morada y los delitos cometidos con ocasión del mismo, pues no cabe hablar aquí de identidad, al menos parcial, de los actos típicos de ejecución de los distintos delitos, sino sólo de coincidencia temporal. El caso más debatido, añade el autor, es aquel en el que el delito permanente sirve de medio para la comisión de otro delito, supuesto para el cual defiende la solución del concurso ideal solo si el delito permanente se concibe, de antemano, orientado a la consecución del hecho criminal posterior, característica intencional ésta recogida en el tenor literal del propio delito permanente (en otro caso no habría coincidencia parcial de la actividad típica ejecutiva, lo que, explica, no sucede en el delito del allanamiento de morada, cuya formulación típica no abarca finalidades ulteriores. Por eso, concluye, en el caso, muy frecuente, en el que el allanamiento de morada aparece instrumentalizado a la realización de otro delito, estaremos ante un concurso real de delitos. Ello sin perjuicio de que pueda venir en consideración, en la situación concreta, la previsión del artículo 77 del Código penal que, como hemos recordado, extiende el tratamiento sancionatorio del concurso ideal a aquellos supuestos en los que una de las infracciones sea medio necesario para cometer la otra. SANZ MORÁN, 2006: 90-92..

que el delito de allanamiento de morada no suele presentarse aisladamente, sino como medio necesario para perpetrar otros delitos[106]. La solución que se debe adoptar, a mi juicio, depende de si se emplea fuerza en las cosas o violencia o intimidación en las personas y de si se trata de un concurso real o ideal:

a) Concurso ideal: utilización de **violencia o intimidación** en las personas habrá que distinguir:

aa) *Vis fisica* ejercida sobre una persona que no tiene la específica función de custodiar el sistema, sino que se encuentra en el lugar donde éste está situado, ello con vulneración posterior de otra medida de seguridad: implicará la aplicación del subtipo agravado de allanamiento de morada previsto en el artículo 202.2 del Código penal.

bb) *Vis fisica* ejercida sobre una persona que tiene como misión la custodia del sistema en tanto medida de tipo organizativo: en este caso, si se castiga la punición de la violencia ejercida sobre la persona que custodia el sistema para apreciar la vulneración de las medidas de seguridad, apreciar esta circunstancia para el allanamiento conduciría a la vulneración del principio *non bis in idem*, de modo que en este caso debería llegarse a la misma solución propuesta para el allanamiento con fuerza en las cosas: un concurso ideal entre el tipo básico del allanamiento de morada del artículo 202.1 y el delito de acceso ilícito del artículo 197 *bis*.

b) Concurso real: no existe ningún género de duda al afirmar que resulta posible un concurso real entre el acceso ilícito cuando no existe conexión directa entre ambos delitos o cuando el allanamiento de morada dura más de lo imprescindible para cometer el acceso.

---

[106] JORGE BARREIRO, 1987: 89.

b) DELITO DE DAÑOS

Por lo que se refiere al delito de daños, con carácter general se estará ante supuestos de unidad delictiva, en los que, a mi modo de ver, el delito de acceso o mantenimiento ilícito desplaza la aplicación del delito de daños[107], desviándose la cuestión al ámbito de la responsabilidad civil derivada del delito, salvo que se sobrepasen los límites de la fuerza necesaria para obtener el acceso[108]. Surge a continuación la necesidad de concretar cuál de los principios informadores del concurso aparente de normas penales debe tomarse en consideración. La solución a esta cuestión en mi opinión es fácil: se aplicará el criterio tercero relativo a la consunción, de manera que, con la salvedad expuesta, los daños quedarán absorbidos por el delito de acceso ilícito[109].

---

[107] El empleo de **fuerza en las cosas** no constituye un elemento del tipo del allanamiento de morada, de modo que la concurrencia de ésta circunstancia con dicho delito daría lugar a la apreciación de un concurso ideal entre el tipo básico del allanamiento de morada del artículo 202.1 y el delito de acceso ilícito del artículo 197 *bis*. Conviene advertir, junto con SUÁREZ MONTES y JORGE BARREIRO, que la violencia integrante del tipo agravado de allanamiento se refiere sólo a la ejercida sobre las personas, de modo que los actos de fuerza sobre las cosas -como es el supuesto de daños causados para introducirse en la morada ajena- no quedan consumidos en el mencionado tipo agravado y estarían en relación de concurso de delitos con el tipo básico o el tipo agravado de allanamiento. JORGE BARREIRO, 1987: 90.. SUÁREZ MONTES, 1968: 900..

[108] Véase la doctrina especializada en materia de robo.

[109] Véase sobre concurso de delitos Sección 1ª del Capítulo V.

C) VULNERACIÓN DE LAS MEDIDAS DE SEGURIDAD

La vulneración de medidas de seguridad es un ingrediente clave para el tipo penal y absolutamente determinante de la conducta típica, pues la vulneración de medidas de seguridad constituye el punto de intersección para la perfección del delito[110]. Efectivamente, la lesión del bien jurídico se produce nada más sobrepasar las barreras de protección establecidas para impedirlo, momento en el que tiene lugar la consumación[111].

No obstante, la decisión acerca de cuando se produce la efectiva vulneración de las medidas de seguridad dependerá, a mi juicio, de tres elementos: la presencia de éstas, su idoneidad y su superación[112]. La conjunción de estos tres elementos permitirá, pues, confirmar la consecución del acceso al sistema y, con ello, constatar un hecho de gran trascendencia para el comportamiento típico: la consumación del delito. Estudiemos cada uno de ellos con detalle:

---

[110] En contra se manifiesta cierto sector y parte de la jurisprudencia italiana, quienes restan importancia a este elemento y consideran que el quebrantamiento de los dispositivos de protección del sistema informático no asume relevancia por sí mismo sino tan solo como manifestación de la voluntad contraria de aquel que dispone del sistema legítimamente, siendo la realización de la contravención de la voluntad del titular, el consentimiento, lo que verdaderamente caracteriza a este tipo penal. Se señala que, de otro modo, debería considerarse atípica la conducta de quien habiendo accedido lícitamente al sistema informático, se mantiene en el mismo en contra de la voluntad del titular. De este modo, la presencia de medidas de seguridad únicamente asumiría relevancia en sí mismo como eventual manifestación de la voluntad contraria de aquel que dispone del sistema de un modo legítimo. Por las razones expuestas a lo lardo del presente Capítulo, esta tesis no puede ser compartida. CUOMO y RAZZANTE, 2009: 101. GAROFOLI, 2013: 644.2. LATTANZI y LUPO, 2010: 1359.

[111] Véase Capítulo IV.

[112] Afirma PLANTAMURA que los índices valoración para entender producida la vulneración deberían atender a la naturaleza y la finalidad de lo accedido, la idoneidad de la intervención a lesionar o poner en peligro los objetivos a los cuales resultaba instrumental la protección del sistema y los datos en él contenido, esto es, la existencia al menos de prohibiciones o límites a conocer o a utilizar los contenidos del área informática accedida, y en fin, las funciones desarrolladas por el sujeto activo en seno a la organización titular del sistema protegido. PLANTAMURA y MANNA, 2007: 46..

1. PRESENCIA DE LAS MEDIDAS

La primera condición a la que me he referido para entender vulnerada la medida de seguridad es la actualidad de la misma, ello en el sentido de que realmente exista algún medio de protección en el sistema, pero también en el de que éste encuentre activo en el momento en el que se produce el acceso. Así pues, debe excluirse la represión penal de la conducta en caso de desactivación o total ausencia de las medidas de seguridad[113]. Dos comentarios al respecto:

a) SISTEMAS SIN MEDIDAS DE PROTECCIÓN

Los sistemas desprovistos de medidas de protección son aquellos sistemas en los que el titular no ha dispuesto ninguna medida de seguridad a efectos de evitar la intrusión o el acceso al mismo por parte de terceros ajenos[114]. Aunque, como se ha indicado anteriormente[115], es posible afirmar la voluntad contraria del titular respecto del acceso a dichos sistemas, lo cierto es que la inexistencia de un mecanismo del protección supondrá el traslado automático del acceso o mantenimiento cometidos contra éstos sin el consentimiento del titular al ámbito de la atipicidad, pues la conducta no podrá ser castigada al no cumplirse uno de los elementos objetivos del tipo. Por tanto, como afirma PICA, aunque sea dudosa la no existencia de una voluntad excluyente del propietario, faltando la instalación de una medida de seguridad, el hecho no será punible[116].

---

[113] Lo anterior aparece muy bien reflejado en el Informe Explicativo del Convenio, donde se afirma la atipicidad de los accesos en los que exista autorización del propietario u otro titular legítimo del sistema, así como de aquellos casos en los que el sistema sea de acceso libre o abierto al público. COUNCIL OF EUROPE, 2001: 14 párrafo 47. PLANTAMURA y MANNA, 2007: 46.

[114] Se discute este término en la No debe confundirse este término con el de sistema abierto, como por ejemplo hace MUCCIARELLI. MUCCIARELLI, 1996: 101. En igual sentido, PICA, 1999: 44.

[115] Véase apartado II. de este Capítulo.

[116] PICA, 1999: 44. En el mismo sentido, BOLEA BARDÓN, 2011: 468. GONZÁLEZ RUS, 2011: 520. MUÑOZ CONDE, 2010: 277-278. QUERALT JIMÉNEZ, 2010: 302. TOMÁS - VALIENTE LANUZA, 2010: 803. CUOMO y RAZZANTE, 2009: 101.

b) ESTADO DE LA MEDIDA EN EL MOMENTO DE LA COMISIÓN DEL DELITO

Una segunda condición indispensable para poder entender culminado este elemento del tipo es la actualidad de la protección, es decir, que la medida de seguridad se encuentre activa en el momento de la comisión del delito a efectos de poder ser superada[117]. En este sentido, el tenor literal del artículo 197 *bis* hace referencia al término *vulneración,* lo que requiere necesariamente la neutralización de los medios de protección que sean necesarios para acceder al sistema[118].

Algunos autores entienden típica la conducta si se verifica una situación de temporal desactivación de las medidas y ésta es abarcada por el dolo del sujeto, por ejemplo, cuando éstas están en proceso de sustitución[119]. Por otra parte, en una interpretación mucho más abierta y, a mi juicio, extensiva y *contra legem*, sostiene otro sector de la doctrina que es suficiente con la mera predisposición de las mismas de manera que quede patente el ejercicio del *ius excludendi* de parte del titular del derecho[120]. Ninguna de estas postulaciones es admisible, de un lado, porque suponen una interpretación extensiva que contradice totalmente el tenor de la ley y sobrepasa *in malam partem* el límite de garantía representado por ésta -si una medida está desactivada, no puede ser vulnerada-, de otro lado, porque se utiliza el elemento subjetivo del tipo para anular un elemento del tipo objetivo[121].

---

[117] AMORE et al., 2006: 106. CERQUA, 2000: 53. PECORELLA, 2011: 5983. RELLA, 2007: 46.

[118] FAVA, 2009: 898.

[119] En este sentido, FLOR, 111; PECORELLA, 2006: 327.

[120] DESTITO et al., 2007: 83. PICA, 1999: 60.

[121] Esta tesis es adoptada por la Corte de Casazione italiana en la Cass. 27. 10.2004 n. 46509 que afirma *per quanto concerne il reato di cui all'art. 615 ter, comma 2, n. 1, CP (capo B) no è ravvisabile la condotta contestata in quanto il sistema informatico nel quale l'imputato si inseriva abusivamente non resulta obiettivamente (ne'la sentenza fornisce la relativa prova) protetto da misure di sicurezza, essendo anzi tale sistema a disposizione dell'imputato in virtù delle mansioni affidategli per ragioni di ufficio. Il fatto che il D.C. ne facesse un uso distorto a fini illeciti e personali, non sposta i termini della questione, mancando il presupposto della "protezione" speciale del sistema stesso. De tale reato pertanto l'imputato debe essere assolto perché il fatto non sussiste.*

2. CRITERIO DE LA IDONEIDAD

El legislador español no ha incluido en el artículo 197 *bis* una previsión expresa acerca de cuáles son los requisitos que las medidas de seguridad del sistema deben cumplir, limitándose a prever la necesidad de su presencia y su destino como barrera frente al acceso: *establecidas para impedirlo*. En Italia, donde ha sucedido lo mismo, la doctrina y a la jurisprudencia han adoptado el criterio de la idoneidad de la medida con la finalidad de determinar cuáles son los medios de protección que realmente se adaptan a dicho fin[122]. Tal fin es también el que justifica el establecimiento de ciertas pautas a modo de condiciones que éstas deben reunir para ser consideradas válidas a los efectos de la aplicación del artículo 197 *bis*, reglas que he ordenado desde un punto de vista cuantitativo y cualitativo.

Sin embargo, debe señalarse que la valoración de los parámetros para valorar como adecuada una medida se debe efectuar a través de criterios puramente objetivos, evitando que dependa de la concreta percepción del sujeto pasivo. A tal efecto, por idoneidad objetiva debe entenderse la vinculación directa entre la medida y el fin de exclusión pretendido[123]. Se ha afirmado, incluso, que dicha idoneidad puede ser, además, potencial[124] siempre que de ella puedan desprenderse signos exteriores del concreto ejercicio del derecho de exclusión de terceros[125].

---

[122] Ello es puesto de relieve por FLOR, 111. CADOPPI et al., 2011: 534. CANNATA, 2006: 534-535.

[123] Los autores que habían vinculado el elemento de vulneración de medidas de seguridad al consentimiento consideran también que el criterio de la idoneidad de la medida debe responder a esta finalidad. Así, TRENTACAPILLI indica que, en un sentido meramente ideal, no solo es una idoneidad a tener lejos eventuales intrusos, cuanto la manifestación del *ius excludendi* titular, atribuyéndole la misma relevancia de la cual goza la violación del domicilio tradicional. TRENTACAPILLI, 2002: 1283. LATTANZI y LUPO, 2010: 1360.

[124] AMORE et al., 2006: 106.

[125] CUOMO y RAZZANTE, 2009: 101.

a) IDONEIDAD CUALITATIVA: COMPLEJIDAD TÉCNICA O EFICACIA DE LAS MEDIDAS

Desde un punto de vista cualitativo deben valorarse dos parámetros: por una parte, el grado de complejidad técnica que debe tener la medida, y, por otro, el nivel de eficacia que debe exigirse a la misma.

1. Complejidad: Considero que siempre que pueda establecerse dicha conexión directa entre la medida y el sistema, generalmente no debe exigirse al titular del sistema la disposición de especiales requerimientos de carácter técnico[126]. Ello con dos excepciones:

aa) Sistemas con deber legal de ultraprotección: la normativa legal prevé en determinados supuestos la necesidad de que ciertos sistema informáticos deban disponer de unos mínimos de seguridad[127]. En este caso, creo que éstos estándares deben haber satisfecho.

---

[126] En general, el grado de complejidad técnica de las medidas de seguridad se considera un aspecto absolutamente irrelevante en la doctrina italiana. Para ella es suficiente cualquier medio de protección o medida de seguridad, aunque sea fácilmente evitable por una persona medianamente experta. Sin embargo, algunos autores aplican erróneamente el criterio de la idoneidad refiriéndolo indebidamente al grado de complejidad técnica y, en este sentido hecho que les conduce a negar la aplicación de este criterio, bajo el argumento de que es suficiente cualquier vía para impedir el libre acceso de terceros, sin la necesidad de que tales cautelas sean efectivamente idóneas para garantizar la *riservatezza* del sistema porque, en su opinión, la norma no hace ninguna referencia a la idoneidad. En el ámbito español, algún autor ha hecho referencia a una idea similar afirmando la necesidad de la proporcionalidad de la medida. En este sentido, QUERALT afirma que el tipo exige un nivel de autoprotección de la víctima, esfuerzo de autoprotección que habrá de ser proporcional a la funcionalidad de su sistema y a la relevancia de los datos que en él se contengan. Sin necesidad de echar a volar la imaginación, resulta que no es lo mismo la protección de una pequeña red doméstica, que la de una asesoría profesional del gremio empresarial, la de un sindicato, la de un banco o la de los cuerpos de seguridad. QUERALT JIMÉNEZ, 2010: 302. AMORE et al., 2006: 106. CUOMO y IZZI, 2002: 101. DESTITO et al., 2007: 83. En contra, BERGHELLA y BLAIOTTA, 1995: 2334. Sobre esta cuestión véase la Sentencia de la Audiencia Provincial de Girona (Sección 4ª) número 358 de 22 de junio de 2015.

[127] ALEO y PICA, 2012: 55.

bb) Sistemas de carácter complejo: Es común en las empresas y, muy específicamente en el ámbito de la Administración pública, disponer de sistemas informáticos de carácter complejo en los que se encuentran instaladas o dispuestas varias medidas de protección con carácter sucesivo a modo de varias capas que permiten modular y graduar el acceso de usuarios a los diferentes niveles. Con ello se pretende proteger mejor el corazón del sistema y la información más confidencial, así como, al mismo tiempo también para ofrecer tipos de servicios públicos de diferente complejidad y coste[128].

2. Eficacia: En general, igualmente, no debe requerirse un determinado coeficiente de eficacia de las medidas de seguridad, únicamente que éstas tengan una eficiencia potencial para el fin pretendido[129]. A tal efecto, no es posible proporcionar ningún parámetro técnico para evaluar dicha eficiencia, ya que ninguno podría considerarse como válido una vez cometida la intrusión[130], a lo que se añade que ningún sistema de seguridad podrá nunca garantizar una seguridad absoluta, a causa de la variedad de riesgos presentes en la actual sociedad del riesgo y de la previsible y siempre creciente agresividad y preparación del criminal informático[131]. Como indica TRENTACAPILLI, una rigurosa interpretación del elemento medidas de seguridad frustraría el intento del legislador y restringiría el campo de los

---

[128] PICA, 1999: 55.

[129] DESTITO et al., 2007: 83. MAIORANO, 2010: 1359.

[130] FLOR y DI LEMBO vinculan erróneamente el criterio de la idoneidad objetiva de las medidas con la idea de eficacia, y así critican la sentencia de ROMA que explico de 4 de abril del 2000, en cuanto a la disposición legal incriminatoria no hace referencia alguna al requisito de la idoneidad de las medidas de seguridad, no impone un estándar de eficacia de la medida de seguridad adoptada. CUOMO, 101. FLOR, 2008: 108. DI LEMBO, 2005: 925 y ss. MAIORANO, 2010: 1360.

[131] CORRERA y MARTUCCI, 1986: 49.

destinatarios del precepto a pocos hábiles conocedores de la tecnología informática capaces de eludir sofisticados sistemas de seguridad, contexto en el cual se acabaría por desconocer la exigencia de la sociedad tecnológica de masa que, en cuanto a tal, es constituida comúnmente de pequeños y medianos usuarios necesitados de eficaces instrumentos de protección[132].

En mi opinión, el grado de idoneidad a exigir por la medida dependerá, además, de las específicas circunstancias del sistema informático y estará relacionado con la tipología de medidas ya estudiadas. Así, desde el punto de vista de la eficacia, creo que las medidas de seguridad deben adecuadas a cada concreto sistema informático, de manera que la protección del sistema debe aumentar o disminuir en idéntica relación a la existencia de una mayor o menor conexión del sistema informático a las distintas posibilidades de red[133].

a) <u>Conexión de área global</u>: en un sistema conectado a una red de área global como puede ser Internet este requisito solo puede ser observado con la instalación de aplicaciones de seguridad lógica (cortafuegos, antiespías, encriptación de la información, uso de contraseñas o claves de acceso…). En

[132] TRANTACAPILLI, Accceso abusivo, 1283. Visto en LATTANZI, 1360.

[133] A favor, GONZALEZ RUS considera que esta exigencia parece oportuna en relación con los accesos que se produzcan a través de la red, pero que no está tan claro, sin embargo, que un criterio así sea correcto cuando se trata de un ordenador no conectado a red alguna y que el intruso se limita a poner en funcionamiento porque no está protegido por clave o contraseña alguna. En este caso, debería entenderse que el simple hecho de mantener apagado el sistema constituye ya una manifestación de la voluntad contraria del titular a que terceros no autorizados puedan acceder al mismo. GONZÁLEZ RUS, 2011: 520..

ningún caso sería suficiente la implantación de medidas de seguridad física[134].

b) <u>Conexión de área local</u>: en un sistema sin conexión de red, basta a mi juicio con la instalación de elementos de seguridad física, como, por ejemplo, una guarda de seguridad o la ubicación en una estancia cerrada con llave o con un cartel en la puerta en el que se especifique privado o reservado.

[134] En este sentido, afirma PICA, que en el caso del acceso abusivo a distancia, la referencia a las medidas de seguridad debe necesariamente leerse en atención a a las medidas de protección de tipo software, propias o internas a la tecnología informática, por definición incorporada al sistema. No obstante, la violación, es decir la superación abusiva, de las medidas software, por cuantos complejos sean, es efectuable sea con accesos físico, es decir obrando directamente sobre la terminal del sistema ajeno, e intentando insertar a medio de ella el código de acceso, como a distancia o de forma remota, por el envío de impulsos por vía telemática PICA, 1999: 53-54.

b) IDONEIDAD CUANTITATIVA

Desde un punto de vista cuantitativo, en general, la especial protección del sistema no debe apoyarse en la cantidad de obstáculos a superar por quien desee cometer la conducta típica, pues la existencia de una sola medida de seguridad puede ser idónea a los efectos de la culminación del tipo[135]. El criterio que regirá en este caso es el de la eficacia antes transcrito: se deberán superar todas aquellas que se hayan dispuesto específicamente para impedir esa concreta modalidad de acceso, lo que puede implicar la neutralización de una sola medida, de una parte de las varias dispuestas o de todas ellas, en función de la configuración de cada sistema informático. A ello no obsta, en absoluto, el género plural empleado por el tenor literal de la Ley para designar las medidas de seguridad. Así pues, aunque a primera vista éste parece referirse a una pluralidad de éstas y no a una sola, es suficiente para integrar el delito la superación de una medida cuando ésta halla sido idónea

[135] Un sector importante de la doctrina italiana se manifiesta también en contra de considerar que deban superarse todos y cada uno de los obstáculos de protección por dos razones: desde un punto de vista formal, afirma que la afirmación individualiza el comportamiento necesario para cometer el delito del cual en el artículo 615 ter CP, pero no agota la categoría del acceso abusivo, debiéndose definir como tal cualquier conducta no autorizada de intrusión o permanencia en un sistema informático ajeno; desde el plano fáctico, el acceso abusivo puede ser cometido también sin la necesidad de una acción de una acción de superación de las medidas de seguridad del sistema (o porque no están activas, o porque el agente está habilitado a introducirse en algún sector transmitiéndole la contraseña idónea, que utiliza para la introducción con el adjetivo de acceder a un sector en el cual carece de consentimiento, o porque el acceso que tienen concedido abarca solamente la realización de operaciones de manutención del software en lugar de tomar conocimiento de los otros contenidos del sistema). A favor, PICA, 1999: 49 nota 17. PICOTTI; PECORELLA En contra, GALDIERI, 2001: 48.

para proporcionar el acceso[136]. En este sentido, la superación parcial de las medidas que no conduzca a la obtención del acceso podrá castigarse solo como tentativa[137].

[136] Ello no sólo porque el plural de medidas de seguridad no indica la necesaria presencia contextual en el sistema de todas las formas de protección posibles sino también porque sólo es indicativo de la abstracta multiplicidad de los medios de protección existente, siendo indiferente que sean aplicados singularmente o cumulativamente. Además, tal limitación de operatividad de la norma iría en contra de la ratio de tutela, incluso de las ordinarias modalidades de agresión a distancia de los sistemas informáticos, que en cambio el legislador bien ha tenido presente. Aunque no lo considero necesario, para vencer esta crítica podría modificarse el tenor literal del precepto, recogiendo la expresión vulneración cualquier género de medida de seguridad establecida para impedirlo, poniéndose el acento no en el número de medidas u obstáculos a superar sino en las consecuencias de tal superación, esto es, en que la medida superada dé acceso libre al sistema. ALEO y PICA, 2012: 53.

[137] Véase Capítulo IV.

Esta misma cuestión se ha planteado respecto del delito de acoso sexual[138],

[138] El artículo 184 relativo al delito de acoso sexual reza: *El que solicitare favores de naturaleza sexual, para sí o para un tercero, en el ámbito de una relación laboral, docente o de prestación de servicios, continuada o habitual, y con tal comportamiento provocare a la víctima una situación objetiva y gravemente intimidatoria, hostil o humillante.* Como puede observarse, el Código penal hace referencia en este precepto al término plural *favores*. En general la doctrina afirma que en el acoso sexual constituye un requisito implícito cierta reiteración de actos, pues la conducta se consuma no con el mero requerimiento de trato sexual, sino que se requiere un resultado concreto que va más allá de la mera solicitud, cual es la creación de una situación objetiva gravemente intimidatoria, hostil o humillante. Suele decirse que con esta expresión el Código penal no se está refiriendo a la solicitud de un único favor, esto es, a una sola solicitud, sino que se exige que los favores sean varios, siendo necesarias varias acciones reiteradas y no una sola, tratándose de un delito de acumulación, hecho que a la postre expresa cierta habitualidad. Tal intelección quizá pudiera apoyarse en la rúbrica del Capítulo referida al acoso sexual, expresión que no aparece en la redacción del tipo, pero que parece implicar esa necesidad de una pluralidad de actos, ya que, de lo contrario, normalmente habría que acudir a la falta de vejaciones injustas. No obstante, literal y tácticamente no puede descartarse que, de forma excepcional, de la intensidad del requerimiento y de las circunstancias pudieran derivarse la existencia del delito, motivo por el cual la doctrina ha ido reduciendo el número de solicitudes de contenido sexual para entender perfeccionado el tipo. Así pues, A pesar de que el Código penal hace referencia a favores de naturaleza sexual, como afirma MUÑOZ CONDE, la solicitud puede ser un acto aislado, aunque el término acoso sexual, que da nombre a este Capítulo, será el resultado de varios actos reiterados de hostigamiento, molestias, etc. acompañados de frases, alusiones o gestos de evidente contenido sexual. Es por ello que doctrina más reciente está admitiendo la existencia de una sola proposición para que surja el tipo, resultando seria y creíble a ojos del sujeto pasjvo. GÓMEZ RIVERO, 2001, 4 y en contra GARCÍA PEREZ, Comentarios, 7. Citados en GÓMEZ TOMILLO, 2010: 733.. La calificación de este delito como un delito de resultado no es una cuestión pacífica. A favor, OTERO GONZÁLEZ, P. El nuevo delito de acoso sexual 538. COBO DEL ROSAL y ZABALA LÓPEZ-GÓMEZ, 2006: 38.. Cierto sector de la doctrina entiende que se trata de un delito de mera actividad, que se consuma con la mera formulación de la solicitud por parte del sujeto activo. Absolutamente convencidos de ello se manifiestan COBO DEL ROSAL y ZABALA LÓPEZ GÓMEZ, quienes opinan que se trata de un delito de amenazas condicionales, en las que la condición es de índole sexual, resultando protegido en él la libertad en la formación de la voluntad de la persona sobre su conducta sexual. Así pues, consideran que, la consumación del delito de acoso sexual se produce con la mera solicitud de favores sexuales sin que sea necesaria ni la provocación de un resultado determinado, ni siquiera la provocación de una situación intimidatoria, hostil o humillante. BOIX REIG, J. y ORTS BERENGUER, E. Consideraciones sobre la… 679. QUERALT JIMÉNEZ: Derecho penal. Parte Especial, Barcelona, Atelier, 2010, pág. 245. COBO DEL ROSAL y ZABALA LÓPEZ-GÓMEZ, 2006: 45 a 50.. QUERALT JIMÉNEZ, 2010: 245.. COBO DEL ROSAL y ZABALA LÓPEZ GÓMEZ se expresan en el sentido de que *la mera solicitud esporádica de un favor sexual no podría constituir, en absoluto, un delito de acoso sexual.* COBO DEL ROSAL y ZABALA LÓPEZ-GÓMEZ, 2006: 54.. GÓMEZ TOMILLO, 2010: 733.. Por último, DE VEGA RUIZ que la primera solicitud debería considerarse inocua, integrando la tipicidad del delito a partir de la segunda solicitud, ello salvo que esa primera vez fuere ya importante, seria, hiriente y humillante. Entonces, entiende el autor, esa única acción quedaría dentro del ámbito de lo punible. DE VEGA RUIZ, 1991: 51., ALTÉS TÁRREGA, 2002: 51.. MUÑOZ CONDE, 2010: 243.. Esta es también la opción mayoritaria defendida por la doctrina laboralista por lo que respecta al ilícito laboral. Así, En el ámbito penal, entre la reciente doctrina MATALLÍN EVANGELIO, A. EL NUEVO DELITO… No obstante, a juicio de NARVÁEZ BERMEJO, con ello se contradice el concepto de acoso, pues éste necesita de una cierta insistencia para que se consume… pág. 92. Sobre acoso sexual en el ámbito laboral véase ALTÉS TÁRREGA: El acoso sexual en el trabajo, pág. 186 y 187.

las insolvencias punibles[139], la usurpación de funciones públicas o el

[139] El párrafo 1º del apartado 1 del artículo 257 del Código penal, relativo a las insolvencias punibles, castiga a quien se alce con sus bienes en perjuicio de sus acreedores, siendo en su día cuestión polémica si debía tratarse de un alzamiento total o era suficiente un alzamiento parcial, más aún, la insolvencia parcial cuando el deudor ha dispuesto de un solo bien. Igualmente, el tipo hace referencia a *sus acreedores* debiéndose aclarar si se trata de o debe tratarse de un solo acreedor o de varios. Como muy bien recogió en su día MUÑOZ CONDE respecto a la antigua redacción del precepto, desde un punto de vista legalista y literal del problema, el Código hace referencia a *sus bienes* en plural. Parece, pues, a primera vista, que se excluye el alzamiento de un bien singular. Pero este argumento no convence al autor, quien acertadamente afirma que se deben más a una forma de estilo que a una razón de fondo. Sus bienes debe interpretarse en relación con alzarse. Alzarse con sus bienes equivale a insolentares y tanto puede insolventarse el que oculta todos sus bienes como el que oculta sólo algunos consiguiendo la insolvencia parcial o el que oculta sólo el único que poseía. Lo decisivo es que se produzca la insolvencia. Esto puede extrapolarse perfectamente al caso del acceso ilícito. Respecto a *sus acreedores* el legislador pudo escoger entre la expresión en singular *su acreedor* o en plural *sus acreedores*, que generalmente se definen como los sujetos pasivos del delito. Eligió esta última por ser más comprensiva, ya que la pluralidad acoge también la unidad, no así el caso inverso. Sin embargo, MUÑOZ CONDE añade en este caso que la expresión en plural tiene también otros alcances que no han sido debidamente precisados hasta ahora. Una de las consecuencias a para el autor de haberse usado la expresión en plural sus acreedores es la de excluir el concurso ideal aunque con el mismo hecho, el alzamiento, se lesione el derecho de crédito de varios acreedores. Afirman ROBLES PLANAS y PASTOR MUÑOZ que se ha criticado con razón, citando a GONZÁLEZ CUSSAC la admisión de la insolvencia parcial como resultado típico, pues o bien el deudor puede hacer frente a su deuda y no hay, por tanto, insolvencia o bien no puede hacer frente a ella y en tal caso concurre insolvencia. En estos casos, se ha hablado de insolvencia parcial en aquellos supuestos en los que el acreedor debe cobrarse con bienes determinados que el deudor hace desaparecer. Sin embargo, tanto doctrina como jurisprudencia han admitido la insolvencia parcial en la medida en que, como afirmaba en su día QUINTERO OLIVARES, si el legislador pretende, entre otras cosas, proteger el respecto a los derechos crediticios de los acreedores, aparecerá como evidente que la efectividad de tal protección debe manifestarse tanto si el ataque se produce contra la total envergadura de su crédito, como si tan sólo se refiere a una parte del mismo, a causa de que el deudor sujeto activo ofrezca en su poder bienes bastantes para hacer frente a un determinado porcentaje. El alzamiento de bienes supone una acción del deudor común que tiene como finalidad frustrar el pago de todas sus deudas, de las que debe responder universalmente con su patrimonio. Debe concurrir el propósito de defraudar a la totalidad de los acreedores. El pago de parte de las deudas, otorgando preferencia a unos sobre otros (acción denominada prelación o preterición de acreedores), impide apreciar el ánimo defraudatorio general, que es el que da vida al tipo penal de alzamiento de bienes (STS 474/2001, de 26 de marzo). MUÑOZ CONDE, 1971: 113, 130 y 131.. Sin perjuicio de alguna voz en contra como CABALLERO BRUN, 2008: 223.. ROBLES PLANAS y PASTOR MUÑOZ, 2012: 259.. FARALDO CABANA, 2010b: 992.. QUINTERO OLIVARES, 1973: 63..

intrusismo profesional[140], con la particularidad de que en esta ocasión se refiere a los medios comisivos.

[140] El artículo 402 castiga como autor de un delito de usurpación de funciones públicas *a quien ilegítimamente ejerciere actos propios de una autoridad o funcionario público atribuyéndose carácter oficial*. El artículo 403, como autor de intrusismo profesional, *a quien ejerciere actos propios de una profesión sin poseer el correspondiente título académico expedido o reconocido en España de acuerdo con la legislación vigente*. Aunque se hace referencia en plural a *actos propio*s, como regla general tanto la doctrina como la jurisprudencia han venido exigiendo para la consumación del delito o bien una sucesión de actos o bien uno solo de especial relevancia. Como afirma QUINTERO OLIVARES, es innegable que el ejercicio de una profesión -con derecho a él o sin ese derecho- pasa por una oferta pública de servicios, que se prestan tantas veces como son contratados o requeridos. Así, como indican COBO DEL ROSAL y QUINTANAR DÍEZ profesionalidad implica habitualidad. De ahí que estos y otros autores hayan sostenido la tesis de que el intrusismo es un delito de caracterizado tal reiteración de actos para entender consumado el delito (dubitativa STS 4 marzo 1988), exigiéndose cierta habitualidad (STS 6 junio 1989 STS 23 de enero de 1984 STS 19 diciembre 1974), entendiendo que supone una interpretación extensiva del tipo que dos actos aislados sean suficientes para integrar la conducta típica. A ello rebate QUINTERO que semejante conclusión no está forzada por la ley, ni siquiera permitida y que el delito podría cometerse con un solo acto de esa naturaleza. Para el autor el problema real se reduce a aceptar que la reiteración de actos en plural está ya prevista por la propia ley, y por lo tanto, el ejercicio habitual de una profesión como intruso no produce tantos delitos como actos profesionales ilícitos, sino un solo delito de ejercicio de una profesión. Por esta razón, la jurisprudencia de la Sala Segunda del Tribunal Supremo ha entendido, en ocasiones, que la actividad puede ser de mero ejercicio continuado pero también de realización de un exclusivo acto de calidad y condición momentánea (STS 18 octubre 1985 y 31 octubre 1986 en la que no se requiere habitualidad siempre que el acto sea idóneo y peculiar de la profesión usurpada). A día de hoy cada vez son más los autores que se pronuncian a favor de considerar la posibilidad de entender consumado el delito con un solo acto. Como afirma MUÑOZ CONDE, es indiferente el número de actos cometidos. Para LLORIA GARCÍA, el delito de intrusismo constituye un supuesto de unidad típica en sentido estricto, en el que, por tanto, los distintos actos constituyen un todo, el ejercicio profesional, por lo que no cabe aplicar las reglas del concurso de delitos, ni del delito continuado (también STC 204/19d96, de 16 de diciembre). El objeto material de delito es la realización o ejecución de actos propios de una profesión para la que sea preciso título oficial, o reconocido por disposición legal o Convenio internacional sin que el texto legal requiera habitualidad, por lo que -cual precisa la STS 3 octubre 1980- tanto puede ser la actividad de mero ejercicio continuado, como de realización de un exclusivo acto de calidad y condición momentánea, siempre que sea idóneo y peculiar de la profesión usurpada, integrando la repetición de de la conducta o su continuidad una misma infracción, sin que puedan estimarse delitos diferentes los actos distintos a ella efectuados a través del tiempo (STS 29 octubre 1992, 30 abril 1994, 29 septiembre 2000, 12 noviembre y 22 enero 2002, 29 septiembre 2006). Para que el delito se consume es necesario que en la acción delictiva el sujeto realice actos propio de una profesión, precisamente del tipo de la profesión usurpada (S 3 marzo 1997). Si bien el delito se consuma con la realización de un solo acto (STS 934/2006, 29 septiembre). El delito -siendo un delito de mera actividad- se consuma con la simple realización de un solo acto propio de la profesión, sin que sea necesaria la habitualidad o repetición de actos, pero en caso de habitualidad hay un solo delito. De hecho requirieron habitualidad las STS 28 marzo 1980, 2 diciembre 1981, 4 marzo 1988 en la que de forma particularmente clara se afirma que es necesaria la habitualidad sobre la base de la redacción en plural del precepto. QUERALT JIMÉNEZ: Derecho penal. Parte Especial, pág. 734. En principio es QUINTERO COBO DEL ROSAL y QUINTANAR DÍEZ: El delito de intrusismo, Madrid, CESEJ, 2006, pág. 91. COBO DEL ROSAL y QUINTANAR DÍEZ: El delito de intrusismo, pág. 92. En sentido similar, SOTERAS ESCARTÍN: Capítulo 5. Falsedades personales, en De las Falsedades. Comentario a los artículos 386 a 403 del Código penal de 1995. Colección de Comentarios al Código penal de 1995 (GANZENMÜLLER ROIG, CARLOS; ESCUDERO MORATALLA, JOSÉ FRANCISCO; FRIGOLA VALLINA, JOAQUÍN (coord. y dir.)), Barcelona, Bosch, 2000, pág. 596 y 597. En el mismo sentido SAP Murcia 5ª 58/2003, 17 de junio. No se entrará a valorar en este trabajo puesto que no es objeto del mismo qué significa un acto idóneo y peculiar de la profesión usurpada. Para ello, puede remitirse el lector a los siguientes trabajos: GÓMEZ MARTÍN, 2011: 884.. LLORIA GARCÍA, 2001: 414.. MUÑOZ CONDE, 2010: 729.. ORTS BERENGUER, 1996, 1772. QUINTERO OLIVARES, 2008, 1582. FARALDO CABANA, 2010a: 1537..

3. SUPERACIÓN DE LAS MEDIDAS

En último lugar, la vulneración de las medidas de seguridad se produce cuando éstas son efectivamente superadas como consecuencia de la voluntad quebrantadora y anulatoria de quien accede ilícitamente al sistema[141]. Ello no significa que deba producirse un menoscabo en el o los elementos de protección del sistema sino que es suficiente con su neutralización debiéndose entender ésta por en el sentido de superación o desactivación temporal[142].

La elusión de la barrera de protección puede provenir de cualquier modo, sea modificando los presupuestos cognoscitivos del software que regula los accesos, como localizando contraseña con repetidas tentativas o rodeando de otra manera la protección del sistema[143]. De este modo, la utilización de la contraseña correcta pero obtenida de un modo subrepticio a través de un previo hurto al titular, de engaño o mediante la utilización de algún tipo especial de software creado al efecto también integrarán este concepto de vulneración.

La exigencia de vulneración de las medidas de seguridad, como se ha visto en el Capítulo correspondiente[144], conduce a la consumación del delito, convirtiendo al acceso ilícito en un delito de resultado por lo que respecta a esta modalidad. Sin ánimo de

---

[141] Véase Capítulo IV.

[142] CADOPPI recoge la primera sentencia en materia de acceso ilícito a un sistema informático dictada en Italia, del Tribunal de Torino de 7 de febrero de 1998, según la cual el artículo 615 ter del Código penal italiano castigaría cualquier introducción en un sistema informático que se realice en contra de la voluntad del titular del derecho, afirmando que para apreciar la intención criminal contraria a tal voluntad se considerará suficiente la superación de cualquier medio de protección que pueda conseguir cualquier persona de capacidad media.

[143] CUOMO, 2000: 101.

[144] Capítulo IV.

reproducir lo ya dicho en el capítulo correspondiente[145], si tan solo se produce la superación de parte de las medidas sin que ello conduzca al acceso libre al sistema o a una parte de él, podrá castigarse como tentativa, pero no como delito consumado. Además, si con la vulneración de una sola medida se obtiene acceso a diversos sistemas informáticos, esto es, a un sistema de información, la conducta se castigará por separado.

[145] Véase Capítulo IV.

CAPITULO VII

EL ELEMENTO NEGATIVO DEL TIPO: LA AUTORIZACIÓN Y VOLUNTAD DEL TITULAR DEL SISTEMA

I. INTRODUCCIÓN

El artículo 197.1 bis contiene una referencia expresa no sólo a la parte positiva del tipo (que se ha estudiado en los capítulos precedentes), sino también a la parte negativa del tipo. De este modo, el tipo penal no se agota con los actos dirigidos al acceso o mantenimiento (desvalor de acción) y el menoscabo del bien jurídico —que se produce con la adquisición de la disponibilidad sobre el sistema y solo en el caso del acceso— (desvalor de resultado), sino que es necesario, además, que el sujeto activo no se halle autorizado para realizar dicho acceso (primer inciso) o que la permanencia en el sistema informático se realice en contra de la voluntad de quien tenga el legítimo derecho para excluirlo (segundo inciso). El último paso que le queda al presente trabajo representará, por tanto, interpretar estas dos expresiones en búsqueda de su significación. Para ello se tomarán como referencia tres parámetros:

> **a) Normativa supranacional:** La Directiva 2013/40/UE del Parlamento Europeo y del Consejo, de 12 de agosto de 2013, explica en el apartado d) del artículo 2 qué debe entenderse por acceso realizado *sin autorización*: *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*. Esta definición debe utilizarse como marco interpretativo del inciso *sin estar debidamente autorizado* al que hace referencia el artículo 197.1 *bis* del Código penal. No sucederá lo mismo, en cambio, en relación con la expresión *en contra de la voluntad de quien tenga un legítimo derecho de exclusión*, pues nada especifica sobre ella la Directiva.
>
> Debe notarse que, al hacer referencia a este elemento típico, ni la Directiva ni el Convenio emplean la traducción exacta en castellano de esta locución, sino que usan la de *without right* (que vendría a significar exactamente sin derecho o más bien ilícitamente). Por las razones que más tarde se expondrán

será necesario analizar la adecuación de la expresión utilizada por el artículo 197.1 *bis* a la utilizada por dicha normativa.

b) Derecho comparado: en segundo lugar se tendrá en cuenta la interpretación que de este elemento ha efectuado la doctrina de los dos países de nuestro entorno que cuentan con una expresión similar, Italia y Francia. Sendos Códigos penales han incorporado este elemento típico aunque con una traducción distinta. Concretamente, Francia ha traducido el concepto *wihtout right* por el de *frauduleusement* e Italia por el de *abusivamente*.

c) Interpretación doctrinal y jurisprudencial de carácter sistemático: la expresión utilizada por el artículo 197 *ter* o expresiones similares (*sin la debida autorización*, *no autorizado legalmente*, *sin estar legítimamente autorizado*, *sin estar autorizado a tal fin*) ha sido utilizada en multitud de tipos penales a lo largo del Código penal. Ello permite también conocer cuál es el sentido y la significación que doctrina y jurisprudencia le han atribuido a los efectos de tomarlos como punto de referencia para colmar el presente análisis.

Teniendo en cuenta estos tres puntos, que informarán el contenido del presente capítulo, éste se estructurará en dos partes: la primera dedicada al estudio de la expresión *sin estar debidamente autorizado* utilizada en el primer inciso del artículo 197.1 bis y la segunda al análisis de la expresión en contra de la voluntad de quien tenga el legítimo derecho de exclusión, a la que hace referencia el segundo inciso de dicho precepto. En cualquier caso, el significado jurídico del concepto de autorización tendrá que estar impregnado por el bien jurídico protegido en el delito de acceso ilícito, la seguridad informática, un valor, como cabe recordar, de naturaleza supraindividual o colectiva que marcará la interpretación de este elemento típico.

II. LA EXPRESIÓN *SIN ESTAR DEBIDAMENTE AUTORIZADO*

Como se ha indicado, el artículo 197.1 bis contiene una referencia expresa no sólo a la parte positiva del tipo, sino también a la parte negativa del tipo, que en la modalidad alternativa del acceso se manifiesta en la expresión *sin la autorización debida*. En efecto, la descripción típica exige conforme a la redacción vigente que el autor acceda al sistema informático sin autorización pero también sin la autorización que sea debida. Se trata de una fórmula polémica que, con expresiones más o menos similares, ha sido utilizada por el legislador español en multitud de tipos penales. Necesariamente, por tanto, han de servir éstos de parámetro hermenéutico para la interpretación de este elemento del tipo, sirviendo para descifrar su naturaleza y contenido.

A) NATURALEZA JURÍDICA: ¿AUTORIZACIÓN COMO ELEMENTO DE LA TIPICIDAD O DE LA ANTIJURICIDAD?

La naturaleza de la autorización ha sido ampliamente discutida en la doctrina, especialmente en sede del Derecho penal medioambiental. Existen al respecto dos posturas que debaten si esta figura conforma un elemento normativo de la tipicidad objetiva[1] o más bien un componente base de la antijuricidad del delito[2].

En mi opinión, el delito de acceso ilícito constituye una **prohibición represiva con reserva de permiso** en la que la autorización cumple la función de convertir en aprobada una conducta socialmente desaprobada como regla general: el acceso a un sistema informático ajeno. En consecuencia, este concepto es expresión de la **antijuricidad** y no de la tipicidad. Ello se fundamenta en dos aspectos[3]:

---

[1] Afirman DOVAL PAIS y ANARTE BORRALLO que, pese a anticipar un elemento característico de la antijuricidad, de él depende la tipicidad. En este sentido, la Sentencia de la Audiencia Provincial de Girona (Sección 4ª) número 504 de 22 septiembre de 2014 (FJ 1º) . ANARTE BORRALLO y DOVAL PAÍS, 2015: 513.

[2] En relación con la naturaleza jurídica de la autorización como causa de justificación, los autores alemanes, quienes de forma más continuada vienen ocupándose de esta cuestión, aparecen divididos. La doctrina dominante considera que estamos ante un caso especial del estado de necesidad, en que afectados varios intereses ha de tomarse partido por el interés preponderante. Se entiende que no existe capacidad de disposición sobre los intereses afectados y que sólo la preferencia de otro interés puede justificar la lesión producida. Otros autores, sin embargo, consideran la autorización como un caso especial del consentimiento y hay quién simplemente reconduce la autorización a la idea de ausencia de interés necesitado de protección. En la doctrina española, el tratamiento de estas cuestiones se ha trasladado fundamentalmente al ámbito de aplicación de lo que en el Código vigente es el actual artículo 20.7, en relación con el ejercicio de un derecho, y a la discusión sobre la posibilidad o no de que la autorización genere un derecho subjetivo relevante en el destinatario de la misma, incluso en casos de autorización ilegítimamente obtenida. En cualquier caso, la principal problemática de esta cuestión surge en el ámbito de la teoría del error. Si se estima que la fórmula comentada expresa un mero elemento normativo del tipo —un presupuesto de la antijuricidad— el error sobre tales extremos sería un error de tipo, mientras que si se interpreta que contiene una valoración que se identifica con el propio juicio de antijuricidad, al pertenecer a ésta y no al tipo, el error sería un error de prohibición En relación con el delito de coacciones, QUINTERO OLIVARES GARCÍA PABLOS DE MOLINA, 140 En relación con coacciones: QUINTERO OLIVARES, 2011: 227-228.

[3] Hacen referencia a ambos aspectos DE LA MATA BARRANCO y DE LA MATA BARRANCO, 2004: 504. LUZÓN PEÑA, 2013:-25.

a) Bien jurídico: la realización de la conducta de acceso ilícito, autorizada o no, supone la afectación del bien jurídico seguridad informática, en relación con la cual existe una prohibición incondicional de lesión. De este modo, la sanción de la conducta de acceso sería la regla general y la autorización representaría el levantamiento excepcional de dicha prohibición y la permisión del ataque a la seguridad informática en base a la primacía que se concede a otro interés contrapuesto a la propia seguridad informática cuya realización es incompatible con su salvaguarda. En consecuencia, con la realización de un acceso vulnerando las medidas de seguridad no se evita la lesión del bien jurídico, sino que únicamente se acepta por ese otro interés preponderante, en base a una decisión, que en favor del solicitante de la autorización toma la autoridad que decide sobre el conflicto de los diferentes intereses contrapuestos, entendida como acto constitutivo y no meramente declarativo del derecho a ejercer la actividad amparada en el permiso[4].

b) Adecuación social: La concurrencia de autorización no convierte el acceso vulnerando medidas de seguridad en una conducta absolutamente normal o adecuada desde una perspectiva social y jurídica[5]. La conducta continúa considerándose desaprobada, siendo la presencia de la autorización la que permite entenderla justificada. En este sentido, un sector doctrinal ha considerado que la mención a la autorización tiene su razón de ser en la mayor frecuencia de los casos en los que habrá de concurrir la justificación de la conducta, hecho que supondría la derogación del principio de regla-excepción que normalmente rige la parte la relación entre la parte positiva y negativa del tipo penal[6].

---

[4] DE LA MATA BARRANCO y DE LA MATA BARRANCO, 2004: 503.

[5] QUINTERO OLIVARES, 2011: 227-228.

[6] MIR PUIG, 294-295.

En consecuencia, la conducta supondrá igualmente la afectación del bien jurídico seguridad informática y seguirá siendo jurídicamente relevante por no ser socialmente adecuada y normal, pero estará excepcionalmente autorizada por la ponderación que la autorización supone de otros intereses concurrentes en el caso concreto.

Esta misma naturaleza se ha atribuido al elemento del tipo equivalente en otros países. Este es el caso de Francia o Italia, que han traducido el concepto *wihtout right* por el de *frauduleusement* y *abusivamente*, respectivamente. Así, por ejemplo, en Italia tanto la doctrina como la jurisprudencia han interpretado este adverbio como expresión de la antijuricidad de la conducta[7]. Cabe recordar que el bien jurídico protegido en el artículo 615 ter del Código penal italiano es el domicilio informático, por lo que tratándose de un bien jurídico personal configura una estructura típica plenamente conforme con la prevista para el delito (basada en el consentimiento), el cual, como cabe recordar, se ha construido en el ámbito italiano a semejanza del allanamiento de morada[8].

[7] Algunos autores (VICARIOLI) consideran que este elemento no conforma expresión de la tipicidad sino de la antijuridicidad general, al entender que el consentimiento es una causa de justificación y no de ausencia de tipicidad. Otros entienden que el adverbio alusivamente introduce una nota de antijuricidad especial que hace que la conducta típica sea difícil de delimitar y que retrasa la declaración de impunidad de un hecho al ámbito de las causas de justificación. CANNATA, 2006: 541-542. MANTOVANI, 2011: 520. PAZIENZA, 1995: 756. PECORELLA, 2011: 5986. PICA, 1999: 51. Véase también FONDAROLI, 1996: 312. MUCCIARELLI, 1996: 100. VICARIOLI, 2008: 246.

[8] CANNATA, 2006: 541.

B) EL CONCEPTO DE AUTORIZACIÓN: PRESUPUESTOS

La tipificación de aquellos accesos que se produzcan en ausencia de la autorización debida presupone que el sujeto activo carece del título jurídico que legitima su acceso[9] en ausencia clara e indudable de permiso suficiente tanto desde una perspectiva objetiva como subjetiva[10]. El delito solo puede cometerse, por tanto, en aquellas situaciones en las que la autorización es necesaria, debiendo existir alguien con capacidad para autorizar en concreto el ejercicio del derecho de acceso[11].

En general, en Derecho penal el concepto de autorización se ha vinculado en el campo de los delitos contra bienes supraindividuales a la noción de *autorización oficial* empleada en el Derecho administrativo, siendo ésta considerada un instituto paralelo al consentimiento del sujeto pasivo en los delitos contra bienes jurídicos individuales[12]. Se trata de lo que la doctrina ha denominado, en ocasiones, accesoriedad administrativa o accesoriedad con respecto a un acto administrativo[13]: la obtención del permiso, consentimiento o anuencia de la autoridad estatal competente, que según los casos será la autoridad administrativa o gubernativa aunque también puede ser la autoridad judicial, es determinante para la realización del tipo[14]. Lo anterior supondría que la plena realización del tipo de injusto sólo se produciría cuando el comportamiento del sujeto lesionase un acto prohibitivo de la autoridad o no estuviera cubierto por un permiso o una autorización administrativa o judicial[15].

---

[9] Respecto de 245.2 Lex Nova, 960.

[10] QUINTERO OLIVARES, 270, 796.

[11] QUINTERO OLIVARES, 270, 796.

[12] Pone de relieve este extremo LUZÓN PEÑA, 2013: 21.

[13]Sobre el particular véase DE LA MATA BARRANCO y DE LA MATA BARRANCO, 2004: 499.

[14] Así la define LUZÓN PEÑA, 2013: 21.

[15] LUZÓN PEÑA, 2013: 21.

No obstante, el contenido que la normativa supranacional atribuye a la autorización en el ámbito del acceso ilícito a un sistema informático no es el mismo que la doctrina atribuye a la autorización oficial. Concretamente, 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, define específicamente el concepto de sin autorización (*without right*, por tanto, en realidad el de ilícitamente[16]), declarando expresamente que se tratará de todo acceso 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*.

Como se observa, de la literalidad de dicha norma se deriva el hecho de que la normativa no sólo está pensando en la autorización oficial, judicial o administrativa, sino también en la autorización de cualquier titular privado que tenga algún género de derecho sobre el sistema, hecho que le otorgaría a éste capacidad para conceder al sujeto un permiso válido para el acceso[17]. En el delito de acceso ilícito, por tanto, la autorización puede ser otorgada, además de por los sujetos enunciados en relación con la autorización oficial, por un particular con algún título jurídico sobre el sistema que le atribuya capacidad para autorizar el acceso. En consecuencia, la noción de autorización tiene un contenido más amplio que la que se venía dando en el ámbito del Derecho penal para los delitos contra bienes jurídicos supraindividuales[18].

---

[16] Véase introducción al presente Capítulo.

[17] Ello vendría corroborado, además, por la tipificación de la conducta de mantenimiento.

[18] Esta es la tendencia que, de hecho, se ha seguido en los demás países. Así, en Francia la Sentencia de la Corte de Apelación de París de 5 de abril de 1994, estableció que el término fraudulento por acceso fraudulento, en el sentido de la ley, debe entenderse cualquier género de penetración irregular de un sistema de tratamiento automatizado de datos: *l'accès frauduleux, au sens de la loi, vise tous les modes de pénétration irréguliers d'un système de traitement automatisé de données, que l'accédant travaille déjà sur la même machine mais à un autre système, qu'il procède à distance ou qu'il se branche sur une ligne de communication*.

Habrá, pues, que determinar ahora respecto del delito de acceso ilícito los presupuestos objetivos de autorización, es decir, en qué casos se puede autorizar, y los presupuestos subjetivos de la misma, esto es, quien puede autorizar.

1. PRESUPUESTOS OBJETIVOS DE LA AUTORIZACIÓN

En primer lugar habrá que concretar los supuestos en los que un sujeto puede autorizar. Aunando por una parte los dos supuestos previstos en la normativa internacional, esto es, la autorización entendida como habilitación legal (*no permitido por el Derecho nacional*) y la autorización, o más bien aquiescencia, del titular del sistema (*no haya sido autorizado por el propietario u otro titular del derecho sobre el sistema o parte del mismo*) y los relativos a la autorización oficial (administrativa o judicial), hallamos tres tipologías distintas de autorización. Los siguientes:

a) AUTORIZACIÓN COMO HABILITACIÓN LEGAL

La primera modalidad de autorización se plantea en aquellos supuestos en los que el sujeto se introduce en un sistema cuyo acceso está vetado por Ley, es decir, *no [está] permitido por el Derecho nacional*. Existe, por tanto, una prohibición legal expresa (una norma de carácter imperativo) que le impide acceder al sistema. En el ordenamiento español, sería un ejemplo el artículo 2 de la Ley 9/1968, de 5 de abril, reguladora de los Secretos Oficiales, que establece que podrán ser declaradas materias clasificadas objetos (entre los cuales se encuentran los sistemas informáticos que contienen los asuntos, actos, documentos, informaciones y datos relativos a la seguridad y defensa nacional) *cuyo conocimiento por personas no autorizadas pueda dañar o poner en riesgo la seguridad y defensa del Estado* y, en relación con los cuales, según el artículo 8, se establece *una prohibición de acceso y las limitaciones de circulación a personas no autorizada*s en locales, lugares o zonas en que radiquen dichas materias clasificadas.

Cabría en este punto plantear si la norma que prohíbe dicho acceso debe o no tener rango legal. Creo que no tiene por qué exigirse tal jerarquía normativa, ya que, por una parte, la propia Directiva no lo establece —es suficiente con que una norma nacional lo prohíba— y, por otra, porque en ningún otro instituto de reenvío penal se exige tal carácter.

b) AUTORIZACIÓN COMO MERA AQUIESCENCIA

En segundo lugar la Directiva explica que el acceso se considerará como no autorizado cuando *no haya sido autorizado por el propietario u otro titular del derecho sobre el sistema o parte del mismo.* No se desprende de la literalidad de la norma ningún requisito a exigir respecto de la autorización el titular deba cumplir, por lo que deberá interpretarse este concepto en un sentido amplio considerándose válido un mero permiso de carácter no formal, verbal o tácito. En cualquier caso, la referencia al propietario u otro titular presupone la posibilidad de que sean varios lo sujetos con capacidad para autorizar. A ello se hará referencia en el próximo apartado.

c) AUTORIZACIÓN OFICIAL

En tercer y último lugar, debe hacerse referencia a la autorización oficial, esto es, aquella concedida tanto en el plano formal (órgano competente) como en el material (acomodo a la legalidad vigente) por cualquier procedimiento de autorización formal que concluya con un acto administrativo o judicial[19]. En este caso habría que plantearse qué ocurriría si, otorgada dicha autorización, se descubre la concurrencia en éste de un vicio invalidante de carácter formal (vicio de procedimiento o del órgano concedente) o material (no se cumplen los requisitos legales exigidos). A ello se hará referencia más tarde[20].

---

[19] Sobre hacking legal, véase ORTIZ PRADILLO, 2011: 67 y ss. ORTIZ PRADILLO, 2012: 177 y ss.

[20] Cuando se comente la expresión debida. Apartado C) de este Capítulo.

2. PRESUPUESTOS SUBJETIVOS: LOS SUJETOS CON POTESTAD PARA AUTORIZAR, ESPECIAL REFERENCIA A LA DIVERSA TITULARIDAD DE DERECHOS

El segundo punto de este apartado pasa ineludiblemente por comentar quién puede autorizar, es decir, cuáles son los sujetos titulares del sistema informático o con algún derecho sobre él que les atribuye la capacidad para poder autorizar válidamente el acceso. Sirva adelantar que, aunque por coherencia expositiva se trate aquí, este comentario resulta trasladable también a la conducta de mantenimiento que, como cabe recordar, se refiere a un conjunto de sujetos con un legítimo derecho de exclusión sobre el sistema (*en contra de la voluntad de quien tenga el legítimo derecho a excluirlo)*. De hecho, es en relación con esta última conducta donde mejor se manifiesta la circunstancia de que pueden ser diversos los géneros de derechos que distintos sujetos ostentan sobre el sistema y que garantizan a sus titulares facultades suficientes para autorizar a un sujeto a acceder o a utilizar legítimamente el sistema informático.

Ahondando en los derechos que dichos sujetos pueden ostentar respecto del sistema informático, se llega a la posibilidad de encontrar no solo varios titulares con algún derecho sobre el sistema sino también titulares con derechos de igual o diferente naturaleza, planteándose como imprescindible la necesidad de ofrecer una solución en caso de conflicto entre ellos. El siguiente paso lo constituirá, por tanto, resolver los conflictos que entre los diversos titulares puedan plantearse. A tal efecto, habrá que escoger entre declarar la igualdad de todos los géneros de titulares de derechos que se proyectan sobre el sistema y, por tanto, establecer una solución conjunta para la prestación de la autorización por parte de todos ellos, o bien crear una prelación entre ellos estableciendo un orden de preferencia en el otorgamiento del mismo.

Debe resaltarse también que sobre este tema no existe pronunciamiento alguno por parte de la doctrina jurídico penal debido a que el tratamiento de la autorización se ha afrontado solo desde la perspectiva administrativa y judicial, donde las respectivas normas jurídicas de cada rama establecen claramente quien es la autoridad con potestad autorizatoria. Nada se ha escrito sobre el particular con capacidad para autorizar en delitos contra bienes jurídicos supraindividuales, pero mucho se ha dicho al respecto sobre su institución paralela en el campo de los bienes individuales, el consentimiento, especialmente en el delito de allanamiento de morada. Acudir a este tipo penal para solucionar los conflictos interpretativos entre distintos titulares me parece adecuado teniendo en cuenta que el principal punto de referencia de la modalidad de mantenimiento es el artículo 615 ter del Código penal italiano y que éste recoge el delito entre los preceptos relativos a la inviolabilidad del domicilio, siendo el mantenimiento el equivalente a la modalidad pasiva de dicho tipo.

En el delito de allanamiento de morada, que he dicho que tomaré como referencia, la doctrina mayoritaria sostiene acertadamente que es suficiente con la autorización de cualquiera de los titulares para permitir la entrada a la morada, de modo que el derecho de admisión o *ius permitendi* corresponde a todos los moradores[21]. A la inversa, en caso de conflicto, se adopta como criterio general el propuesto por RODRÍGUEZ DEVESA, hoy seguido por la mayor parte de la doctrina, que supone la aplicación de la máxima latina *iusprivatista* de condominio *melior est conditio prohibendi*, según la cual debe prevalecer la voluntad prohibitiva sobre la que manifiesta anuencia[22].

---

[21] BOLEA BARDÓN, 2011: 477. CARBONELL MATEU y GONZÁLEZ CUSSAC, 2010: 1016. JAREÑO LEAL, 2010: 477. MORALES PRATS, 2010: 513-514. MUÑOZ CONDE, 2015: 288. NÚÑEZ CASTAÑO, 2010: 238. QUERALT JIMÉNEZ, 2010: 285.

[22] BOLEA BARDÓN, 2011: 477. CARBONELL MATEU y GONZÁLEZ CUSSAC, 2010: 1016. JAREÑO LEAL, 2010: 477. MORALES PRATS, 2010: 513-514. MUÑOZ CONDE, 2015: 288. NÚÑEZ CASTAÑO, 2010: 238.

En coherencia con lo anterior, en general la doctrina defiende que resulta indiferente el **título jurídico** que ostenta cada uno de los titulares[23] (siendo suficiente con que éste sea legítimo[24]), afirmando que se trata de una situación fáctica y que lo único relevante es la vulneración del bien jurídico[25]. A mi parecer, este criterio puede sostenerse hasta cierto punto, ya que su aplicación categórica podría conducir a la sin razón de afirmar que un menor de edad tiene la posibilidad de negar la entrada a alguien en el domicilio en contra de la voluntad de sus padres. Creo que es por ello que cierto sector de la doctrina ha limitado dicho criterio, aplicándolo a salvo de las prelaciones que pueden inferirse del *ius corrigendi* o de la situación jurídica en que se encuentren los distintos moradores[26].

---

[23] La razón por la que se argumenta en este sentido responde a la aparente dificultad que podría presentarse para determinar quién es el sujeto pasivo, ello en la medida en que sobre la morada pueden recaer distintos títulos, facultades o relaciones de carácter jurídico, que pueden dar legitimidad para consentir o no la entrada o permanencia en ella. Afirma en este sentido HERNÁNDEZ PLASENCIA que, tratándose el allanamiento de morada de un delito que atenta contra un bien personalísimo como la intimidad y no contra el patrimonio o derechos de naturaleza económica, el concepto de morador no se determina en función de un título de naturaleza jurídico económica que pueda recaer sobre el objeto material del delito. Por tanto, dicho autor distingue de los moradores, sujetos pasivos del delito, a otros sujetos que tengan facultades jurídicas de disposición sobre la morada, pero que no son titulares del bien jurídico lesionado sobre la base de que, para ser sujeto pasivo, es suficiente que se ostente una facultad para excluir a terceros de la morada, como podrían ser el amigo o el administrador al cuidado de la vivienda cuando sus moradores están fuera. Por tal motivo, para el autor, deben quedar amparados sujetos cuya intimidad puede verse afectada, aun careciendo de título jurídico que ampare la habitación en la morada, citando, a modo de ejemplo, las situaciones de precariedad. En definitiva, para él, el dato que permite identificar al sujeto pasivo del delito es la habitación efectiva en la morada, pero sin perjuicio de que pueda concurrir, a su vez, títulos jurídicos de naturaleza patrimonial o civil, pero éstos, por si solos, son insuficientes.

[24] Afirma JORGE BARREIRO que la legitimidad del uso de la morada podrá consistir en una relación jurídica formal (propiedad o arrendamiento) o en una mera situación de hecho reconocida por el Derecho (como la de precario). JORGE BARREIRO, 1997: 598.

[25] A favor, BOLEA BARDÓN, 2011: 477. JAREÑO LEAL, 2010: 477. JJORGE BARREIRO, 1997: 596. QUERALT JIMÉNEZ, 2010: 285. NÚÑEZ CASTAÑO, 2010: 238.

[26] CARBONELL MATEU y GONZÁLEZ CUSSAC, 2010: 1016.

Teniendo en cuenta la naturaleza mucho más compleja del acceso ilícito, considero oportuno en aras a la seguridad jurídica tener en cuenta el título jurídico de los sujetos para dirimir quien tiene un mejor derecho y así establecer un orden de prelación entre los distintos títulos[27]. Además, la doctrina acude ya a las prelaciones que se infieren del *ius corrigendi* o de lo que califica como situaciones jurídicas de los distintos titulares[28], lo que, en definitiva, no supone más que tener en cuenta la relación jurídica existente entre ellos.

Concretamente, la solución correcta por lo que a mí respecta implica, primero, resolver los conflictos producidos entre sujetos con un distinto título jurídico y, después, aportar una solución cuando éstos se producen entre titulares de un mismo título, porque, como indica la máxima constitucional, para supuestos de hecho iguales las consecuencias jurídicas han de ser iguales, mientras que para supuestos de hecho diferentes las consecuencias jurídicas han de ser diferentes. Presento, pues, este desarrollo:

> **a) Si la naturaleza de los títulos jurídicos de los diversos titulares es distinta**, entonces me parece adecuado establecer una prelación entre ellos, suscitándose entonces cuál debe ser el orden más ajustado a Derecho. Dejando de lado ciertas opiniones un tanto arcaicas y, en ocasiones, incluso discriminatorias, no me parece en absoluto deleznable defender la existencia de una posible jerarquía ni en el ámbito del allanamiento de morada ni en el ámbito del acceso ilícito tanto en el ámbito familiar como en el laboral o de recreo.
>
> En tales casos, debe darse preferencia al criterio de quien ostenta la posición jurídica (que no fáctica) preeminente dentro del grupo porque así se desprenda *ex vi legis*[29], ello

---

[27] Por esta solución optan GONZÁLEZ RUS, 2011: 338. JORGE BARREIRO, 1987: 76. JORGE BARREIRO y RODRÍGUEZ MOURULLO, 1997: 601.

[28] CARBONELL MATEU y GONZÁLEZ CUSSAC, 2010: 1016. MORALES PRATS, 2010: 513-514.

[29] GONZÁLEZ RUS, 2011: 338.

siempre con la susodicha limitación de que no se lesione o ponga en peligro la libertad correspondiente a los demás miembros del grupo[30]. JORGE BARREIRO, que considera casi imposible dar una fórmula exacta que pueda resolver todos los conflictos, distingue particularmente en el ámbito del allanamiento de morada dos situaciones que me parecen de sumo interés y que considero también plenamente adaptables al delito de acceso ilícito a un sistema informático[31]:

> **1. Convivencia total o parcialmente jerarquizada:** (conventos, familias con personal doméstico etc.), donde los derechos de admisión y exclusión corresponderán, en principio y con carácter general, al jefe o cabeza del grupo, que lo ejercita personalmente o mediante persona en quien delegue. Entretanto, los sujetos subordinados ostentan un derecho de exclusión con respecto a extraños y sólo en relación a los espacios reservados para el propio y exclusivo uso (habitaciones) y una limitada facultad de admisión por tácita delegación con respecto a los lugares comunes.
>
> **2. Convivencia familiar:** en la cual no suscribe el principio de quien prohíbe tiene mejor derecho, pues únicamente la prohibición de uno o ambos padres tendrá prioridad cuando la entrada pueda lesionar la intimidad familiar. Es hoy doctrina unánime que en el caso de los menores que autorizan la entrada a los amigos en contra de la voluntad expresa de los padres, debe prevalecer la voluntad de éstos.

---

[30] SUÁREZ MONTES, 1968: 885.

[31] JORGE BARREIRO, 1987: 76-77, JORGE BARREIRO, 1997: 601.

b) Si la naturaleza de los títulos jurídicos de los distintos titulares es la misma, se ofrecerá una solución una vez resueltos los conflictos derivados del apartado anterior. Se trata, en este caso, de solventar las discrepancias surgidas entre iguales, esto es, cuando son varias personas quienes ostentan un título jurídico de la misma especie y calidad sobre el sistema informático. POLAINO NAVARRETE, ante la igualdad de derechos de los moradores en el deltio de allanamiento de morada, propugna los criterios de la adecuación social de la conducta y de la integración social del grupo familiar para determinar los bienes preponderantes, atendiendo a los hábitos personales y familiares, las costumbres sociales, la ubicación del lugar de la morada, la cronología de los acontecimientos sociales, etc.[32]. Esta solución, normalmente cajón de sastre para las cuestiones de difícil resolución en el ámbito penal, me parece excesivamente genérica para este supuesto, donde se pueden ofrecer criterios más claros en aras a la seguridad jurídica. En mi opinión, en el acceso ilícito destacan dos grupos de supuestos:

> **1. Sistema informático de titularidad múltiple dividido en compartimentos estancos:** En los casos en los que del mismo sistema sean titulares varias personas del que se hayan dividido compartimentos estancos (como sucede en el caso de los pisos compartidos), entonces cualquiera de ellos puede autorizar el acceso o mantenimiento a la parte del sistema que tiene atribuida, pudiendo el tercero acceder a aquellas partes del sistema que sean comunes sin que los restantes titulares puedan negarse a ello[33].

---

[32] POLAINO NAVARRETE, 1997: 447.

[33] Respecto de allanamiento de morada véase SERRANO GÓMEZ y SERRANO MAÍLLO, 2011: 294.

2. Sistema informático de titularidad múltiple sin división en compartimentos estancos: en este caso sí que considero oportuno aplicar el principio general de que cualquiera de los titulares puede emitir un permiso válido a efectos de permitir el acceso porque el derecho de admisión o *ius permitendi* corresponde a todos los titulares, pero en caso de conflicto *melior est conditio prohibendi,* debe prevalecer la voluntad prohibitiva o *ius prohibedi* sobre la que manifiesta anuencia[34].

Por último, debo puntualizar que el orden de prelación establecido en este segundo punto no debe considerarse de carácter absoluto, sino que es necesario atender al caso concreto para poder ofrecer una solución completamente ajustada a Derecho. En este sentido, creo que lleva mucha razón cierto sector doctrinal al advertir que ofrecer una solución con una pretensión global puede ser arriesgado debido a que puede dar cobijo a decisiones arbitrarias o de abuso de Derecho. Es por ello que considero que resultará necesario ponderar todos los elementos en juego y, muy especialmente, observar cuál es la posibilidad de afectación concreta para cada uno de los titulares[35] a efectos de valorar hasta qué punto la autorización dado por parte de alguno de ellos hace comprensible la conducta del sujeto o no, pudiendo crearse una situación de no exigibilidad de una determinada conducta.

---

[34] Esta es, de hecho, la opción adoptada por la jurisprudencia para resolver los supuestos de existencia de un vínculo de afectividad entre los titulares en el allanamiento de morada.

[35] Así como propone JORGE BARREIRO y SANZ MORÁN dicho principio general ha de someterse en Derecho penal a las oportunas restricciones, pues tal tesis no será siempre defendible, como sería el caso de que la conducta de quien prohíbe suponga un abuso de derecho respecto de los legítimos derechos de los demás moradores. REBOLLO VARGAS, 2004: 492-493. En el mismo sentido MUÑOZ CONDE, 2015: 287. HERNÁNDEZ PLASENCIA, 2004: 886.

C) EL ADVERBIO "DEBIDAMENTE"

1. SIGNIFICACIÓN JURÍDICA

El artículo 197.1 *bis* no establece únicamente que la conducta se haga sin autorización, sino que requiere, concretamente, que se trate de la autorización *debida*. Precisado el concepto de autorización se presenta ahora la necesidad de ofrecer significación al término que lo acompaña. La inclusión de este adverbio (o del adjetivo debida) —y, con ello, la de la propia referencia al concepto de autorización[36]— no es en absoluto superflua ya que hace referencia a que la autorización de la que dispone el sujeto debe ser válida jurídicamente, hecho que supone mantener la tipicidad de aquellos supuestos en los que existe una autorización oficial fáctica pero ésta no es plenamente válida en el plano jurídico[37].

En consecuencia, cuando concurre la autorización debida, plenamente válida jurídicamente, para llevar a cabo el acceso al sistema, dicha autorización excluye toda la antijuricidad de la conducta. Así pues, la ausencia de autorización relevante para el Derecho penal no puede integrarse simplemente con una autorización dada por alguien que sobrepasaba su título o autorización, o con una duda sobre el alcance de la autorización[38]. Todas esas situaciones, y otras muchas parecidas, tienen su adecuado campo de discusión en el proceso civil[39].

---

[36] La doctrina no coincide en cuanto a la necesidad y acierto de su mención, ya que mientras por una parte se ha considerado que se trata de una remisión superflua debido, me imagino, a que dichas causas de exclusión de la antijuricidad se aplican con carácter general para todos los delitos RAIGUÉS I VALLÉS (SILVA SÁNCHEZ)

[37] En contra de esta opinión, GUARDIOLA LAGO afirma que la expresión debida permite, por tanto, incluir tanto los comportamientos en los que no existe autorización para el acceso como aquellos otros en los que existe autorización, pero que exista algún vicio en ella por alguna de las siguientes razones: ser manifiestamente contraria a Derecho, que el otorgante careciese de competencia o que la autorización hubiera sido concedida al margen del procedimiento formal marcado por la Ley que hubiera debido seguirse al respecto. GUARDIOLA LAGO, MARIA JESÚS, 590, 2291. LUZÓN PEÑA, 2013: 23.

[38] QUINTERO OLIVARES, 270, 796

[39] QUINTERO OLIVARES, 270, 796

2. ¿ACCESORIEDAD DEL DERECHO PENAL?

Exigir una autorización jurídicamente válida implica tener en cuenta por parte del Derecho penal la normativa administrativa o de la correspondiente rama jurídica extrapenal a los efectos de determinar cuando la conducta está legalmente autorizada y cuando no. Ello hace surgir la idea de que en este caso sí que rige la accesoriedad del Derecho penal respecto del Derecho administrativo y/o las restantes ramas del ordenamiento jurídico, en coherencia con el principio de unidad del ordenamiento jurídico y la ausencia de contradicciones entre sus diversas ramas para la permisión o juridicidad de la conducta[40].

Ahora bien, como indica LUZÓN PEÑA, la validez de la autorización no es incompatible con alguna irregularidad jurídica no invalidante, o sea que las que no provocan ni siquiera la anulabilidad del acto administrativo, en este caso, la autorización, o con algún pequeño vicio invalidante en las otras ramas del Derecho[41]. Sobre cuáles son esas meras irregularidades no invalidantes, o sea, que no producen nulidad ni anulabilidad, hay que esperar a lo dispuesto en el Derecho administrativo o, cuando se trata de autorizaciones judiciales, en el Derecho procesal[42].

[40] LUZÓN PEÑA, 2013: 27.

[41] LUZÓN PEÑA, 2013: 27.

[42] LUZÓN PEÑA, 2013: 27.

D) LA EXPRESIÓN *WITHOUT RIGHT* EN LA NORMATIVA SUPRANACIONAL Y LA INTERPRETACIÓN DEL ARTÍCULO 197.1 *BIS* CONFORME A LA MISMA

Una vez analizado el contenido y alcance del término autorización tanto desde una perspectiva objetiva como subjetiva, es necesario examinar si la significación ofrecida cumple las expectativas de la normativa supranacional que, como cabe recordar, utiliza la locución *without right*, la cual vendría a significar exactamente sin derecho o ilícitamente. Se hace necesario determinar, a continuación si es correcta la referencia que efectúa el artículo 197.1 bis a la autorización o más bien debiera utilizar otro término y si esta expresión se adecua a la empleada por la Directiva y el Convenio.

Antes que nada es necesario poner de relieve, como ya se anunció en la parte introductoria de este Capítulo, el por qué de tanto hincapié en la necesidad de este examen. Pues bien, tal y como se indicó en el Capítulo I[43], el Informe *Computer-related crime – analisys of legal policy* de 1986, de la Organización para la Cooperación y Desarrollo Económico hacía referencia al término sin autorización (*without the authorization*) en el acceso ilícito. Posteriormente, sin embargo, la Recomendación 89 (9), del Consejo de Europa, adoptada el 13 de septiembre de 1989, sobre delincuencia informática, sustituyó dicha expresión (*without the authorization*) por la de sin derecho (*without right*) —cuya ajustada traducción al castellano sería a mi juicio, más bien, ilícitamente—. La razón de dicha sustitución estribó en la idea de que esta última locución tiene un contenido más amplio y permite subsumir un mayor número de actuaciones injustas en la descripción típica, como, por ejemplo, el incumplimiento de una relación contractual o también los casos en que la prohibición de acceso se deriva de una disposición legal imperativa además de aquellos en los que éste depende de la voluntad dispositiva del usuario legítimo del sistema.

[43] Véase Capítulo I.

Esta nomenclatura ha sido mantenida en la versión inglesa de toda la normativa internacional y comunitaria dictada desde entonces en la materia y es, de hecho, la que utilizan el Convenio sobre Cibercriminalidad, de Budapest el 23 de noviembre de 2001 y 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[44].

Cabe plantearse, por tanto, si el alcance del término autorización (solo del término autorización porque la conducta de mantenimiento no está prevista en la normativa supranacional) tal y como éste está descrito en el artículo 197.1 bis del Código penal es susceptible de dar cobijo a todas las acepciones expuestas, en el sentido de permitir entender incardinada en ella, por una parte, la facultad de exclusión que en relación con el acceso atribuye la normativa supranacional al titular del sistema informático o a cualquier otro sujeto con algún derecho sobre éste y, por otra, los supuestos de acceso que tienen lugar en contra de las previsiones legales aprobadas con la finalidad de establecer una prohibición de acceso respecto de determinados sistemas informáticos. En cualquier caso, también deberá examinarse si a la finalidad planteada —la

---

[44] En este concreto apartado el Informe Explicativo del Convenio puntualiza que el término ilegítimo debe ser interpretando en el plano del contexto en que se plantea la posible ilicitud del acceso, de tal forma que –sin pretensión de restringir la aplicación de este concepto por parte de los Estados conforme a su Derecho interno– entiende que deben resultar incardinables en él todas aquellas situaciones en las que el acceso se lleva a cabo sin tener facultades para ello (ya sean de orden legislativo, ejecutivo, administrativo, judicial, contractual o consensual) o en ningún modo amparado por justificaciones, excusas y defensas legales establecidas o por principios pertinentes con arreglo a las leyes nacionales. A tal efecto, indica que el Convenio no afecta a las conductas legítimas de un Gobierno cuando éste interviene para mantener el orden público, proteger la seguridad nacional o investigar los delitos, ni a las actividades legítimas y comunes inherentes al diseño de las redes o a prácticas comerciales que no deben ser consideradas delitos como es, en este caso concreto, los enlaces de hipertexto, incluidos los cookies, que permiten el acceso a una página web. COUNCIL OF EUROPE: Explanatory Report to the Convention on Cybercrime, 2001, disponble en: http://conventions.coe.int/treaty/en/reports/html/185.htm. 12 y 14 párrafos 38 y 48. Para más información véase Capítulo I.

subsunción de todos estos supuestos— responde mejor la utilización de otro término, como es el caso de Italia o Francia[45].

Aunque ésta es una cuestión que ha pasado desapercibida para la doctrina, la denominación de este elemento típico sí que ha sido comentada en la jurisprudencia. Ésta la ha concebido como un término equiparable al adverbio ilícitamente, que utiliza con mayor frecuencia, y al que ha atribuido un contenido prácticamente idéntico al planteado en el apartado relativo a los presupuestos objetivos de la autorización, englobando, de hecho, al amparo de este concepto todos los supuestos planteados[46].

En mi opinión, por tanto, el término autorización debe interpretarse en el sentido de quedar englobados los dos aspectos que en la normativa internacional se prevén: aquellos supuestos en los que lo único que se está infringiendo es el tenor de la ley, la *voluntad legis* en tanto previsión de una conducta prohibitiva de acceso, y aquellos casos en los que la infracción proviene del propio consentimiento del titular en tanto voluntad de permiso o aceptación de la conducta llevada a cabo por un particular para que el sujeto realice una conducta típica. Sin embargo, teniendo en cuenta la estrecha vinculación entre el concepto de autorización y el Derecho administrativo —vinculación que ha sido puesta de relieve en el presente estudio—, me parece más apropiado utilizar el término ilícitamente que el de sin la debida autorización.

---

[45] Véase Apartado II A) in fine de este Capítulo.

[46] Como indico, la jurisprudencia utiliza la expresión autorización e ilícitamente de forma similar. Así, en materia de coacciones, la Sentencia del Tribunal Supremo 626/2007, de 5 julio establece que el acto debe ser ilícito -sin estar legítimamente autorizado- será examinado desde la normativa que la regula y que la ilicitud de acto se debe examinar desde la perspectiva de las normas referentes a la convivencia social y al orden jurídico. Sobre la misma temática y también en un sentido similar se expresa la Sentencia del Tribunal Supremo 628/2008, de 15 de octubre. La Sentencia del Tribunal Supremo 723/2008, de 10 de noviembre, añade a ello que ausencia de autorización se suele entender existe cuando no concurre una eximente de justificación y que es frecuentemente el ejercicio de un derecho o el cumplimiento de un deber.

II. LA EXPRESIÓN *EN CONTRA DE LA VOLUNTAD DE QUIEN TENGA UN LEGÍTIMO DERECHO A EXCLUIRLO*

A) LITERALIDAD

Antes que nada, creo necesario hacer una referencia a la literalidad de la expresión *en contra de la voluntad de quien tenga el legítimo derecho a excluirlo*. Como se observa, el Código penal hace referencia al titular o titulares del sistema evitando así acoger arcaicas expresiones que se recogen en otros preceptos del Código, como la tradicional referencia al dueño de la cosa.

La utilización de esta expresión permite la subsunción en el tipo de todos los supuestos que deben serlo, salvando así los problemas interpretativos que pudiera causar el empleo de otras locuciones como la de titular del sistema o la malograda alusión al dueño que aparece en otras infracciones penales de entre las cuales el ejemplo más destacable lo constituye el delito de hurto[47]. El uso de cualquiera de ellas en el delito de acceso ilícito impediría, a mi juicio, castigar multitud de conductas que se realizan con la autorización de un titular de un derecho distinto a la propiedad sobre el sistema, por ejemplo, la cesión momentánea de un mero derecho de uso, o a penar injustamente un hecho legitimado conforme al Derecho civil. La única forma de salvar este escollo supondría efectuar una interpretación analógica a favor del reo al igual que sucede en el delito de hurto, algo que no es necesario gracias a la corrección del tenor literal de la Ley.

---

[47] En el delito de hurto, por ejemplo, el problema surge cuando el sujeto pasivo, esto es, el tenedor de la cosa es una persona diferente del dueño, y además ésta ignora que éste haya dado su consentimiento o, no ignorándolo, entiende que ese permiso no podía darlo por afectar a los derechos que como poseedor o tenedor le corresponden. El consentimiento del dueño en este caso solamente despliega su eficacia cuando es efectivamente éste el que tiene en su poder la cosa, o cuando teniéndola persona diferente, ésta también consiente, si es que se ha percatado del apoderamiento. Es por ello que tanto doctrina como jurisprudencia entienden que en el delito de hurto debe considerarse dueño toda aquella persona que ostente un título jurídico sobre la cosa que le legitime a permitir que otro la tome. GILI PASCUAL y MONTSERRAT SÁNCHEZ-ESCRIBANO, 2014: 20. QUINTERO OLIVARES, 2008: 620. QUINTERO OLIVARES, 2007: 478.

B) CONTENIDO

Tal y como se ha indicado anteriormente, el segundo inciso del artículo 197.1 bis, relativo a la conducta de mantenimiento, no hace referencia al concepto de autorización sino que utiliza la expresión *en contra de la voluntad de quien tenga el legítimo derecho para excluirlo*. La literalidad de esta expresión proviene del artículo 615 ter del Código penal italiano, que, como se ha repetido en diversas ocasiones, incrimina este delito entre los tipos relativos al allanamiento de morada.

En el apartado anterior se ha comentado el común alcance de esta expresión con la de *sin estar debidamente autorizado* que recoge el primer inciso del artículo 197.1 bis al estudiar los presupuestos objetivos y subjetivos de la autorización. Ahora, por tanto, resta analizar si en cuanto a contenido puede existir alguna diferencia entre una y otra.

En el ámbito del allanamiento de morada (de donde es oriunda esta expresión) se discute si este elemento significa que la acción típica se dirige inmediata y exclusivamente en contra de la voluntad del afectado, es decir, que para la comisión del delito no es suficiente con la ausencia sin más de la autorización del titular del derecho, ni tampoco con la presunción de voluntad contraria, sino que debe constar una voluntad contraria del titular real, existente y manifestada explícitamente a la realización de la acción típica[48]. Esta postura se fundamenta en la idea de que la locución *en contra* no resulta equiparable a la preposición *sin* puesto que en ella se contiene un mayor contenido de injusto que se manifiesta en la existencia de un contraste efectivo de voluntades entre el autor y el titular[49]. En este sentido se señala que este conflicto de voluntades es el que justifica la inclusión de este elemento del tipo, cuya mención sería

[48] MUÑOZ CONDE, 2015: 258.

[49] SUÁREZ MONTES, 1968: 880.

superflua si su función fuera meramente la de poner de manifiesto la ausencia de autorización[50].

Esta tesis no es compartida por la mayor parte de la literatura jurídica sobre la materia, y tampoco puede ser aceptada por lo que respecta al acceso ilícito. La aplicación de este criterio implica entender que cualquier persona ostenta un derecho de acceso o de mantenimiento sin restricciones sobre el sistema informático hasta que uno de sus titulares manifieste expresamente su oposición al mismo[51]. La solución correcta en mi opinión es la inversa, es decir, entender que existe, por tanto, una presunción *iuris tantum* y *erga omnes* de voluntad contraria del titular[52], en el sentido de que cualquier introducción o permanencia debe entenderse como prohibido siendo la autorización del titular la que justifique para ese supuesto concreto la conducta[53]. Habrá que atender, por tanto, a la voluntad del sujeto que accede o se mantiene en el sistema informático, voluntad que, por otra parte, pertenece únicamente al tipo subjetivo[54]. Lo anterior nos conduce a afirmar que la expresión en contra de quien tenga un legítimo derecho de exclusión y sin estar debidamente autorizado como frases sinónimas. En consecuencia, a ambas expresiones debe atribuírsele idéntica significación.

---

[50] SUÁREZ MONTES, 1968: 880.

[51] JORGE BARREIRO, 1987: 66. SUÁREZ MONTES, 1968: 881. GÓMEZ PAVÓN, 1989: 936.

[52] JORGE BARREIRO, 1987: 66.

[53] SEGRELLES DE ARENAZA distingue entre dicho conflicto de voluntades en el allanamiento de morada activo y el pasivo: En el activo, afirma, la voluntad contraria es fácil de determinar, puesto que, salvo una autorización expresa o tácita del morador, la entrada estará prohibida. En el allanamiento pasivo, puesto que la regla general es que quien se encuentra en morada ajena lo está con consentimiento del morador, es preciso exigir algo más que su ausencia, y por eso el tipo utiliza la frase contra la voluntad que expresa la necesidad de un acto de oposición que, en esta ocasión, no se podrá presumir. SEGRELLES DE ARENAZA, 2000: 312.

[54] JORGE BARREIRO, 1987: 66. SUÁREZ MONTES, 1968: 881. GÓMEZ PAVÓN, 1989: 936.

CONCLUSIONES
Y
PROPUESTAS DE *LEGE FERENDA*

I. A nivel supranacional la persecución y punición del acceso ilícito a un sistema informático ha sido considerada una cuestión de primer orden. Así pues, la necesidad de tipificar la conducta de acceso ilícito a un sistema informático se ha manifestado como una constante a lo largo de las tres últimas décadas en el ámbito supranacional, dirigiéndose todas las iniciativas a conseguir una sanción armonizada cada vez más agresiva.

En el Capítulo I ha quedado patente como esta conducta fue uno de los primeros comportamientos informáticos cuya incriminación se reclamó por parte de las distintas instancias internacionales. Efectivamente, el acceso ilícito constituyó a nivel supranacional una de las primeras conductas cuya punición se propuso en el momento en que la delincuencia informática podía considerarse, todavía, un fenómeno incipiente. Corroboración de lo anterior lo constituye su inclusión en el primer instrumento adoptado con el cometido de ofrecer una respuesta penal a esta fenómeno delictivo: el Informe *Computer Related-Crime: Analysis of Legal Policy* de la Organización para la Cooperación y el Desarrollo Económico de 1986.

Posteriormente, esta necesidad de tipificación se ha mantenido inalterada en las sucesivas disposiciones que las organizaciones de carácter supranacional han adoptado en la materia con el fin de conseguir el principal objetivo marcado en este ámbito: la armonización de la legislación penal de los Estados. En cada uno de los textos adoptados la incriminación del acceso ilícito se ha mantenido entre los actos "mínimos" cuya punición ha sido considerada vital para la protección de los múltiples intereses vinculados a la informática. Y no solo eso, sino que los elementos típicos del delito se han visto prácticamente inalterados a lo largo de las distintas disposiciones que se han aprobado con dos excepciones dirigidas a arbitrar una mayor represión de la conducta. La evolución incriminatoria ha tendido, pues, a reducir los elementos a exigir desde un punto de vista objetivo, ampliando el ámbito típico hacia

una mayor inclusión de comportamientos posibles, siempre, eso sí, que la intención subjetiva del autor quede patente y que la acción de acceso sea dolosa. Se ha vetado, por tanto, la cabida de la imprudencia. Esta ampliación del contenido típico puede observarse:

a) En la primera formulación de la descripción típica, donde el elemento relativo a las medidas de seguridad formaba parte de los elementos integrantes del tipo objetivo. Posteriormente, sin embargo, se consideró que el mero acceso ilícito al sistema, con independencia de que se hubiesen o no vulnerado medidas de seguridad, ya constituía una conducta con el suficiente desvalor como para ser sancionada penalmente. Así, la exigencia relativa a la vulneración de medidas de seguridad se concibió como una posibilidad facultativa para los Estados, junto con la cual se previeron otras tantas tanto en el plano objetivo como subjetivo. Lo anterior supone una ampliación considerable del marco represor.

b) En segundo lugar, también en la expresión del término "sin derecho", que podría traducirse al castellano como "ilícitamente", cuyo contenido resulta circunscrito en primer lugar al tenor de la ley y después al consentimiento del propietario del sistema informático.

Asimismo, la conducta también ha sido deslindada respecto de otras, poniendo de manifiesto que no es necesaria la provocación de interferencias o de repercusión alguna en el funcionamiento del sistema informático, así como tampoco implica el uso del ordenador por quien accede ilícitamente a él. Por este motivo, han sido eliminados determinados requisitos objetivos que han ampliado la conducta hasta las máximas posibilidades de incriminación. No obstante, esta ampliación se ha visto, en todo caso, limitada por el carácter doloso de la conducta.

Finalmente, se han aprobado dos textos vinculantes con el cometido de crear una legislación uniforme en materia de ciberdelincuencia, siendo la primera de las conductas cuya incriminación se propone la relativa al acceso ilícito a un sistema informático. Dichas normas son el Convenio sobre Cibercrimen de 23 de noviembre de 2001 del Consejo de Europa y la Directiva 2013/40/UE del Parlamento Europeo y del Consejo, de 12 de agosto, relativa a los ataques a los sistemas de información y por la que se sustituye la Decisión Marco 2005/222/JAI, de 22 febrero. De ello se desprenden las siguientes conclusiones:

a) La conducta de acceso ilícito debe ser incriminada como delito en todos los Estados miembros de la Unión Europea y en todos los Estados parte del Convenio sobre Cibercrimen de 2001. El fin que persigue la aprobación de la normativa supranacional es el acercamiento de la normativa nacional de los Estados de manera que exista una regulación concreta para el acceso ilícito en cada uno de ellos.

b) Para la consecución de dicho objetivo la Directiva y el Convenio establecen una regulación de mínimos, es decir, recogen los elementos indispensables que deberán integrar la tipicidad de la conducta, debiendo los Estados adoptar las medidas necesarias para incorporarlos a su ordenamiento jurídico. En este caso, para cada Estado pueden darse dos posibilidades:

1. Que ya tenga incorporada la conducta en su ordenamiento nacional como consecuencia de la transposición de alguna de las normas recomendatorias aprobadas con anterioridad a la Directiva y al Convenio. En este caso, el legislador estatal deberá valorar si la infracción penal vigente en su normativa nacional se adapta a las exigencias supranacionales y, en caso de que no sea así, modificar su legislación a los efectos de cumplir las expectativas supranacionales.

2. Que decida incorporarla *ex novo* a su ordenamiento jurídico, hecho que puede tener lugar de dos formas: mediante la aprobación de legislación especial o también a través de su incorporación en el respectivo Código penal del país, ya sea como un tipo de equivalencia o como un tipo autónomo.

c) El Convenio otorga a los Estados una mayor libertad para la conformación del tipo (al igual que hacía la Decisión Marco), pero la Directiva restringe considerablemente la libertad de actuación de los Estados. El Convenio opta por diseñar un marco típico extenso y que deja a los Estados la decisión sobre si estrecharlo o no. Desde esta perspectiva, la uniformidad perseguida por la Unión Europea permite una efectiva aproximación de las legislaciones nacionales, mientras que la del Convenio se aleja mucho de este propósito en la medida en que las variaciones que pueden existir en las fórmulas que se hayan introducido en uno y otro Estado pueden variar sustancialmente.

d) Ninguna de las normas supranacionales impide que, respetando el mínimo indicado, los Estados puedan ampliar la protección prevista en la norma. Puesto que la regulación recogida en ésta es, como se ha dicho, una regulación de mínimos.

II. Desde la perspectiva nacional, la transposición de las normas mencionadas (Directiva y Convenio) se ha realizado en la práctica totalidad de los Estados miembros de la Unión Europea y también en los Estados parte en el Convenio sobre Cibercriminalidad.

De los sesenta y cinco países que son miembros del Consejo de Europa o de la Unión Europea o que, no siéndolo, han firmado o ratificado el Convenio sobre Cibercrimen, cuarenta y nueve han tipificado como delito en sus respectivas legislaciones el acceso ilícito a un sistema informático. Solo un Estado miembro de la Unión Europea no ha aprobado todavía normativa de transposición (Suecia) así como únicamente cuatro Estados miembros del Consejo de Europa no son parte en el Convenio (Mónaco, Rusia, San Marino y Ucrania). En cambio, siete países que no son miembros del Consejo de Europa ni de la Unión Europea sí son parte en el Convenio y han aprobado normativa de transposición de éste (Australia, Canadá, Estados Unidos de América, Filipinas, Japón, Islas Mauricio y República Dominicana).

De todos los países a los que se ha hecho referencia, tan sólo diez (Albania, Bélgica, Canadá, España, Estados Unidos de América, Francia, Italia, Luxemburgo, Moldavia y Turquía) han introducido también como modalidad alternativa el mantenimiento ilícito en el sistema informático.

Por lo que se refiere al objeto material, principal incongruencia de la reforma de 2010 en España, treinta y tres han adoptado como tal el sistema informático o conceptos que pueden considerarse equivalentes (sistema de tratamiento automatizado de datos: Francia, Holanda, Letonia, Luxemburgo, Suiza y Turquía) o una aproximación a éste (ordenador en el caso de Estados Unidos de América, Irlanda, Japón, Islas Mauricio, Montenegro, Serbia, Sri Lanka, Reino Unido y la República de Macedonia, o computer service en el caso de Canadá), mientras que sólo quince han protegido el contenido de éste, esto es, los datos (Alemania, Armenia,

Australia, Austria, Bulgaria, Croacia, Grecia, Islandia, Malta, Moldavia, Noruega y Serbia) o la información (Azerbaiján, Dinamarca y Eslovaquia), y únicamente cinco (Eslovenia, Hungría, Lituania, Polonia y República Dominicana) han optado por utilizar la nomenclatura de la Directiva, que alude a sistema de información.

En cuanto a los elementos que el Convenio recoge como facultativos para los Estados, son dos los que se ha optado por introducir:

a) El relativo a la vulneración de las medidas de seguridad, que han incluido como parte del tipo objetivo un total de veintidós países (Albania, Alemania, Andorra, Armenia, Australia, Austria, Azerbaiján, Bosnia y Herzegovina, España, Estonia, Estados Unidos de América, Finlandia, Hungría, Italia, Japón, Letonia, Lituania, Montenegro, Noruega, Polonia, Serbia y Suiza). Aunque en el ámbito de la Unión Europea la incorporación de éste elemento en el tipo penal nacional de transposición de la Directiva 2013/40/UE es obligatoria, ya que como se ha visto en esta norma este elemento forma parte de la legislación de mínimos, son diecisiete los países que castigan el mero acceso ilícito a un sistema sin necesidad de que se vulneren medidas de seguridad (Bélgica, Bulgaria, Chipre, Croacia, Dinamarca, Eslovaquia, Eslovenia, Francia, Grecia, Holanda, Irlanda, Luxemburgo, Malta, Portugal, Rumanía, Reino Unido y República Checa). Esto significa que la mayor parte de países consideran una conducta de suficiente entidad el mero acceso a un sistema informático

b) y la finalidad de obtener datos, que únicamente ha introducido tres Estados (Moldavia, Reino Unido y República de Macedonia). Otros pocos países han exigido la finalidad de causar un perjuicio (Eslovaquia, Irlanda, Reino Unido y República Dominicana) y/u obtener un beneficio (Austria, Eslovaquia y Irlanda).

III. La conducta de acceso ilícito a un sistema informático fue incorrectamente transpuesta en el Código penal español pero la descripción típica ha sido notablemente mejorada en 2015.

La Ley Orgánica 5/2010, de 22 de junio, introdujo el acceso ilícito a un sistema informático mediante la formulación de un tipo de equivalencia con el delito de descubrimiento y revelación de secretos, concretamente en el apartado 3 del artículo 197 del Código penal. Para lograr una adecuada conexión entre la conducta que en tal momento se introducía y los dos apartados que la precedían —los tipos básicos de descubrimiento y revelación de secretos— el legislador español se vio obligado a modificar los términos de la descripción típica propuesta por la normativa supranacional, incluyendo elementos distintos a los previstos en ella. De este modo, en lugar de incriminarse el acceso ilícito a un sistema informático, en realidad, el introducido apartado 3 no hacía más que castigar una nueva modalidad de descubrimiento y revelación de secretos.

En 2015 la conducta ha sido modificada, se mantiene en el mismo Capítulo relativo al descubrimiento y revelación de secretos, pero deja de ser un tipo de equivalencia para constituir un tipo autónomo en el seno del mismo Capítulo, siendo trasladado del apartado 3 del artículo 197 al apartado 1 del artículo 197 *bis*, precepto de nueva creación por parte de la Ley Orgánica 1/2015. Ello permite una nueva interpretación de los elementos del tipo más adaptada a las pretensiones de tutela.

IV. El bien jurídico protegido ha variado con cada una de las reformas del Código penal, siendo susceptible, tras la reforma de 2015, de ser concebido de una forma más amplia y, por tanto, más ajustada a la pretensión de tutela contenida en el Convenio y la Directiva.

Con la reforma de 2010 el bien jurídico protegido no podía ser otro que la intimidad. Ello por tres motivos: la ubicación sistemática del precepto entre los delitos contra la intimidad, la formulación del nuevo delito como un tipo de equivalencia con los dos tipos básicos

del delito de descubrimiento y revelación de secretos y su necesaria integración sistemática con los dos apartados precedentes para dilucidar su ámbito aplicativo. Así pues, teniendo en cuenta que para configurar el apartado 3 el legislador había tomado como punto de referencia los dos tipos básicos que le precedían, esto es, el apartado 1 y 2 del artículo 197, el interés jurídico a proteger no podía ser distinto al tutelado en éstos.

Tras la reforma de 2015, la conducta se mantuvo en el mismo Capítulo relativo al descubrimiento y revelación de secretos, pero dejó de ser un tipo de equivalencia para constituir un tipo autónomo en el seno del mismo Capítulo, siendo trasladado del apartado 3 del artículo 197 al apartado 1 del artículo 197 *bis*, precepto de nueva creación por parte de la Ley Orgánica 1/2015. Ello permite desligar el acceso ilícito de la intimidad a los efectos de concebir una pretensión de tutela más amplia vinculada a la seguridad informática.

Aunque con mucho ahínco se ha buscado por parte de la doctrina española y comparada la identificación concreta de un objeto jurídico que ligara adecuadamente las pretensiones de la necesidad de tutela planteada y aunque tampoco se ha podido llegar a un acuerdo unánime en la doctrina y la jurisprudencia al respecto, lo cierto es que en las distintas posturas que se han barajado al respecto tienen un fundamento similar, centrado en los posibles peligros que las nuevas tecnologías pueden entrañar a través de la realización de distintas acciones humanas, las cuales pueden generar riesgos tanto de carácter individual como colectivo para los usuarios, ahondando así en una de las características que mejor definen el Derecho penal de la sociedad de riesgo, la tutela del pacífico disfrute de las actividades que rodean los actuales focos de riesgo estabilidad. En este sentido, la desconfianza y el uso pacífico y sin cortapisas constituyen, en definitiva, caras opuestas de una misma moneda, la seguridad informática, siendo éste el bien jurídico protegido en el delito de acceso ilícito.

La seguridad informática se instituye como un nuevo bien jurídico supraindividual cuyo surgimiento se justifica en la idea de que la única manera de defender el interés personal de los propietarios de los sistemas es a través de la salvaguarda de un bien común: la confianza en la utilización lícita de las nuevas tecnologías. En consecuencia, ésta conforma un derecho de titularidad colectiva y carácter puro que comprende el ejercicio de determinadas condiciones se seguridad para el funcionamiento de sistemas y para el goce tranquilo de determinados derechos o bienes individuales a modo de barrera de protección para éstos, que se encuentran mediatamente protegidos por aquella.

Desde esta perspectiva, el acceso ilícito se presenta como el delito básico contra las amenazas y ataques a la seguridad informática, puesto que pretende proteger a los usuarios legítimos de los sistemas informáticos contra las intromisiones que puedan conducir potencialmente a la comisión de ulteriores ilícitos con un mayor contenido de injusto. Tutela, claramente, un bien jurídico de carácter supraindividual con referencia a otros bienes jurídicos, hecho que no obsta, como he dicho, para afirmar su autonomía. Al bien jurídico supraindividual, la seguridad informática, se le dispensará una tutela inmediata, mientras que el resto de intereses serán protegidos en el delito de forma mediata.

Ello significa que, concretamente, se trata de un delito de los denominados de lesión-peligro en el que se distingue, por un lado, la lesión de un bien jurídico de carácter colectivo o supraindividual, la seguridad informática, y, por otro, en la medida en que éste se configura en relación con bienes individuales, la afectación de estos últimos quedaría limitada a una situación de peligro.

Además, la seguridad informática es un interés jurídico plenamente integrable en la Constitución, concretamente en su artículo 18.4 que afirma *pleno ejercicio de sus derechos.* Y como todo interés jurídico puede atribuírsele en cuanto a contenido una vertiente negativa y otra positiva:

a) Desde una perspectiva positiva, la seguridad informática implica un derecho a poder ejercer el disfrute de la informática como ciudadano libre.

b) Desde una perspectiva negativa, implica salvaguardar un ámbito de no interferencia en el uso de la informática por parte de los poderes públicos y de los ciudadanos.

Desde esta perspectiva, el acceso ilícito debería introducirse como una nueva categoría dentro de los delitos contra la seguridad colectiva ya que con ello se atendería mejor a su naturaleza.

IV. A) La Ley Orgánica 5/2010, de 22 de junio, al introducir la conducta en el seno del artículo 197, previó un tipo mixto alternativo compuesto por dos acciones con distinto objeto material: el acceso a datos o programas contenidos en un sistema informático o en parte del mismo, y el mantenimiento en dicho sistema en contra de la voluntad de quien tenga el legítimo derecho a excluirlo. B) Con la Ley Orgánica 1/2015, de 30 de junio, el delito de acceso ilícito ha sufrido una reestructuación por lo que respecta a sus elementos típicos. La reforma operada Ley Orgánica 1/2015, de 30 de marzo, ha mantenido inalteradas ambas conductas, pero ha añadido una nueva modalidad alternativa de comisión del delito, la facilitación del acceso, y ha modificado el objeto material del delito, que ahora es el sistema informático (sistema de información) para todas las modalidades típicas y que será objeto de comentario en el próximo apartado.

El acceso se introdujo *ex novo* a través de la Ley Orgánica 5/2010, de 22 de junio como un nuevo apartado 3 del artículo 197 del Código penal, previéndose en su descripción un tipo mixto alternativo compuesto de dos conductas: el acceso a datos o programas contenidos en un sistema informático o en parte del mismo, y el mantenimiento en dicho sistema en contra de la voluntad de quien tenga el legítimo derecho a excluirlo. Sin embargo, el objeto material del delito era distinto en cada conducta.

A través de la reforma operada por la Ley Orgánica 1/2015, de 30 de marzo, esta incongruencia típica se ha corregido, siendo hoy en ambas conductas el sistema informático el elemento sobre el que recae la acción. Hoy se trata, como anuncia el propio tipo al incluir la conjunción disyuntiva "o", de un tipo mixto alternativo cuya culminación tendrá lugar cuando se produzca cualquiera de las dos acciones que en él se describen —esto es, tanto la de acceso como la de mantenimiento—.

1. La primera de las dos conductas castigadas en el artículo 197.1 bis es el acceso o la facilitación del mismo al conjunto o a parte del sistema informático —acceso a datos o programas contenidos en todo o en parte de un sistema informático según la redacción vigente entre 2010 y 2015—. Como bien se observa, en esta modalidad comisiva la acción típica viene determinada por el verbo acceder, habiendo sido elevados a la categoría de autoría los casos de participación (facilitación del acceso), lo que supone una clara ampliación de la propuesta prevista en la normativa supranacional.

El acceso debe entenderse como una intrusión de carácter electrónico por parte del sujeto activo en un sistema informático ajeno a través de la realización en el mismo de operaciones no consentidas por el titular. Se trata, efectivamente, de una introducción electrónica en el sistema, ya que para culminar dicha injerencia en el sistema ajeno resulta indispensable no sólo el mero contacto con el hardware del sistema, sino también la iniciación de un diálogo activo con el software, siendo esto último —el diálogo con el software— el elemento fundamental e indefectible que permite concluir la efectiva realización del acceso. El hecho de que el objeto material protegido sea el continente y no el contenido conduce a excluir cualquier tipo de toma de conocimiento sobre los datos como elemento del tipo. Acceder excluye de todo punto la obtención del control sobre los datos en el sentido que exige el apoderamiento. Acceder al sistema implica mera introducción sin posesión y sin conocimiento.

La Ley permite dar una cobertura igualitaria y global a todas los posibles ataques contra el bien jurídico protegido, esto es, tanto a los ataques de tipo físico como a aquellos que se producen de forma remota, así como aquellos que tienen lugar de forma parcial como total al sistema. En cualquier caso, lo importante en ambos supuestos es reseñar que el tenor literal del precepto no se está refiriendo a la totalidad acceso al contenido del sistema, lo que no concordaría en ningún caso con el perfil jurídico-interpretativo que se ha presentado en el presente estudio, retrotrayendo el momento de la consumación a un momento posterior.

La consumación del delito requiere, en mi opinión, haber sobrepasado las medidas de seguridad. Para lograr lo anterior, el sujeto activo deberá superar cuantos medios de protección, físicos o lógicos, le impidan iniciar el diálogo con el sistema, puesto que el tipo penal solo ofrece protección a los sistema informáticos dotados de medidas de seguridad (recuérdese que el acceso debe producirse vulnerando las medidas de seguridad).

La superación de tales medidas otorga al sujeto la disponibilidad sobre el sistema, situándole en la condición de acceder u obtener los datos, informaciones y/o programas eventualmente almacenados en el sistema o en alguna parte de éste, y produciéndose la perfección del delito sin que sea necesaria mayor incursión o interrupción en su funcionamiento.

Desde esta perspectiva, el delito se configura como un delito de resultado y no de mera actividad, en el que, tras la desactivación o superación de las medidas de seguridad, el sujeto logra una incursión electrónica en el interior de la memoria interna del sistema obteniendo la disponibilidad sobre el mismo.

Desde este punto de vista, el acceso ilícito se configura también, como un delito de consumación instantánea en el que la perfección se produce en el momento y lugar del acceso, y de efectos prolongados, pues sus efectos se prolongan hasta que el sujeto activo abandona el sistema informático.

En cuanto a la tentativa, en España se regirá por las reglas generales, lo que implica al tratarse de un delito de resultado que ésta será plenamente admisible. En este sentido, todas aquellas acciones que se produzcan en un momento anterior a la adquisición de la disponibilidad sobre el sistema supondrán una imperfecta realización del tipo caerán en el ámbito de la tentativa, acabada o inacabada.

Constituirá tentativa, pues, el simple contacto del sujeto activo con el sistema, así como la superación parcial de las medidas de seguridad, sean éstas lógicas o físicas. En este sentido, en relación con las medidas de tipo físico dispuestas únicamente en el local pueden resultar conflictivos aquellos supuestos en los que tiene lugar la mera introducción de la persona en el lugar donde se encuentra el sistema informático, caso en el que deberá atenderse al criterio de la idoneidad objetiva que más tarde se expondrá. Además, puesto que el objeto material del delito es el sistema informático y no los datos informáticos, el hecho de que el sistema informático esté vacío o que los datos que en él se encuentren estén protegidos no alterarán la consumación del delito, pues el sujeto ya ha adquirido la disponibilidad del sistema.

2. La segunda de las dos conductas castigadas en el artículo 197.1 bis es el mantenimiento en el sistema informático en contra de la voluntad de quien tenga el legítimo derecho a excluirlo. Esta conducta está castigando, en realidad, el mero uso ilegítimo del sistema informático. Concretamente, en ella son susceptibles de tener cabida cuatro modalidades: el abuso modal o temporal del acceso concedido, los supuestos de revocación de la autorización tras un acceso autorizado, el acceso involuntario o casual con mantenimiento doloso y los supuestos de acceso excepcional. Además, a diferencia del acceso, se configura como un delito de mera actividad que se consuma con la simple permanencia y de carácter permanente, puesto que sus efectos se prolongan hasta el abandono del sistema por parte el sujeto activo.

Debe reseñarse que el elemento relativo a las medidas de seguridad con el que el artículo 197.1 *bis* encabeza su enunciado debe vincularse únicamente al acceso, eliminándose cualquier tipo de conexión entre éste y la conducta de mantenimiento. Ello porque la *ratio* de la incriminación en la permanencia ilícita se cimienta en la idea de que resulta necesario ofrecer protección al titular del sistema también en aquellos supuestos en los que la lesión del bien jurídico se deriva del hecho de que el sujeto activo ya se encuentra en el interior del mismo como consecuencia de un acceso previo lícito. En este sentido, la previsión típica de esta conducta debe permitir arbitrar una protección global al sistema frente a los peligros que puedan dimanar no ya de quien accede ilícitamente a él *ab initio*, acto que sería ya castigado al amparo del acceso, sino del comportamiento de quien, inicialmente autorizado, pone en peligro el bien jurídico protegido por el delito.

Desde esta perspectiva, este comportamiento típico adquiriría mayor coherencia si el legislador español le hubiera otorgado el mismo sentido legislador italiano le confirió al incriminar el acceso ilícito en el seno de los delitos de contra la inviolabilidad del domicilio y al considerarla una conducta atentatoria contra el domicilio informático. En este caso sí que cabría distinguir una modalidad de carácter activo, el acceso, y una modalidad de carácter pasivo, el mantenimiento en el sistema. No obstante, la coherencia que el mantenimiento ostenta en el ordenamiento italiano, en el que ambas conductas están adecuadamente ubicadas entre los delitos contra la inviolabilidad del domicilio, se pierde en el ordenamiento español, donde resulta distorsionada en tanto en cuanto si éste hubiera sido el deseo del legislador, la hubiera incluido en el Capitulo II del Título X y no en el Capítulo I, pues la inviolabilidad del domicilio se ha configurado como un derecho autónomo de la intimidad tanto a nivel constitucional como en el ámbito penal.

En cualquier caso, la punición del mero uso del sistema resulta muy criticable desde la perspectiva de los principios de ofensividad y de intervención mínima. La conducta debe destipificarse,

considerándose, por tanto, irrelevante desde la perspectiva penal debido a que no puede entenderse que afecta al bien jurídico protegido por el tipo penal, por la escasa gravedad de la misma. No obstante, entretanto, el juzgador, teniendo en cuenta que cualquier uso no autorizado del sistema informático queda normalmente incluido en aquella descripción, deberá excluir a través de una motivada interpretación restrictiva de la norma en sintonía con el principio de mínima intervención los usos de sistemas informáticos de menor gravedad en los que no haya sido suficientemente afectada la seguridad informática en aplicación del principio de insignificancia.

V. De entre las distintas modificaciones que la Ley Orgánica 1/2015 ha llevado a cabo, la más sustancial ha sido la relativa al objeto material del delito, que es ahora el sistema informático.

A) En el 2010, la conducta que fue objeto de incriminación en el Código penal español tomó como objeto material los datos informáticos (datos contenidos en todo o en parte de un sistema informático) en una clara equivalencia con los dos tipos básicos recogidos en los artículos 1 y 2 del artículo 197, —con el matiz de que el apartado 1 también hace referencia a elementos materiales como cartas, papeles u otros documentos contenidos en soporte físico—. Sin embargo, a diferencia de los dos apartados anteriores del precepto, que sí establecían características delimitadoras de los datos a los que ofrecían protección, en el caso del nuevo apartado sólo se exigía que los datos se hallaran contenidos en todo o en parte de un sistema informático. Esta característica resultaba también predicable de los dos apartados anteriores y no permitía deslindar el recién introducido apartado de sus predecesores.

A tal efecto, para delimitar su ámbito aplicativo era necesario efectuar una delimitación más precisa de los datos que se tutelaban en él. Para ello, debían seguirse los siguientes pasos:

a) En primer lugar, debía fijarse qué es lo protegido en cada uno de los apartados del artículo 197, determinándose con exactitud

qué eran datos de contenidos en efectos personales, datos de las telecomunicaciones, datos personales automatizados y datos personales especialmente protegidos.

b) Una vez establecida la premisa anterior, podía delimitarse con precisión cuáles eran los concretos datos protegidos en cada uno de los párrafos del artículo 197 y, con ello, conocer las lagunas existentes a lo largo del articulado del precepto antes de la introducción del apartado 3 por parte de la Ley Orgánica 5/2010, de 22 de junio.

Las operaciones reseñadas conducían, finalmente, a llenar de contenido el introducido apartado 3, que se configuraba como un tipo residual, esto es, un cajón de sastre al amparo del cual castigar todas las conductas contra la intimidad que no era posible sancionar en aplicación de los demás apartados. Daba cobijo, pues, a las siguientes ilícitos:

a) Accesos no calificables como apoderamiento respecto de los objetos materiales especificados en el apartado 1 del artículo 197 de acuerdo con la interpretación realizada en el presente estudio sobre el concepto de apoderamiento.

b) Apoderamiento o acceso a datos de terceros, en la medida en que el artículo 197.1 exige que los datos objeto de apoderamiento o acceso sean del titular del soporte objeto de apoderamiento y del titular de los datos informáticos (doble titularidad), de modo que, si los datos apoderados pertenecen a un tercero, la conducta no entra dentro del ámbito típico del apartado 1 del artículo.

c) Acceso a datos personales no reservados a los que se refiere el apartado 2 del artículo 197.

d) Acceso a datos que no sean registrados en ficheros informáticos tal y como exige también el artículo 197.2.

e) Acceso a datos que no sean personales o familiares, aunque no deben excluirse de inicio ningún tipo de datos, resultaba difícil encontrar un dato que no fuera personal y contuviera o fuera reflejo de la intimidad de la persona, pues un dato que no sirve para poder identificar a una persona tampoco puede ser reflejo de su intimidad.

En cuanto a la delimitación positiva del concepto de dato, la más adecuada era la definición supranacional, definición plenamente válida para poder definir el concepto de dato informático contenido en un sistema informático, siempre que no se olvidase la mención de los siguientes elementos de interpretación:

1. Bien jurídico: puesto que el artículo 197.3 tenía como objeto de protección la intimidad o, más bien la privacidad, la definición de dato debía vincularse a ésta.

2. Elemento negativo de la definición: no podía olvidarse en la definición de dato la puesta en relación de este apartado con los apartados 1 y 2 del artículo 197 pues el apartado 3 conformaba un tipo residual de los restantes apartados del precepto cuyo ámbito típico debía fijarse en atención a una delimitación sistemática negativa.

En consecuencia, los datos informáticos ex artículo 197.3 del Código penal serían aquel conjunto de informaciones, hechos o representaciones de la privacidad susceptibles de tratamiento automatizado a través de la utilización de un sistema informático, excluidos los datos informáticos protegidos en los apartados 1 y 2 del artículo 197.

Como se ha visto, la configuración del objeto material tras la introducción del delito por medio de la reforma operada por la Ley Orgánica 5/2010, de 22 de junio, era una de las principales incongruencias típicas a resaltar en la infracción penal. En este sentido, la previsión de un objeto material distinto, unida a la ubicación sistemática del precepto, además se suponer un

incumplimiento de la normativa supranacional, planteaba multitud de conflictos interpretativos, entre ellos el relativo a la delimitación del alcance y contenido del objeto material del delito. Así pues, acertadamente, el legislador ha modificado a través de la reforma operada por la Ley Orgánica 1/2015, de 30 de marzo, tanto la ubicación sistemática del precepto como el objeto material de la conducta de acceso, que ahora es el sistema informático en ambas modalidades típicas.

Esta modificación del objeto material ha dotado de una mejor coherencia al tipo, que ahora, efectivamente, es un tipo mixto alternativo en el que ambas acciones comparten un objeto material común, y, además, ha supuesto la mejor adaptación del mismo a las exigencias derivadas de la normativa supranacional, puesto que se han solventado los problemas derivados del hecho de que el acceso a un sistema informático puede implicar no solo el acceso a datos sino también a otros componentes del mismo, a los que se estaba vetando cualquier tipo de protección con una previsión típica únicamente vinculada al concepto de dato.

No obstante, en la actual redacción vigente del artículo 197.1 bis no se hace referencia directa al sistema informático, sino al sistema de información. Ello es consecuencia del acogimiento de la terminología usada por la Directiva, 2013/40/UE, de 12 de agosto de 2013, del Parlamento Europeo y del Consejo, relativa a los ataques contra los sistemas de información y por la que se sustituye la Decisión marco 2005/222/JAI del Consejo, herencia de ésta última, en lugar de la del Convenio sobre Cibercrimen de Budapest, de 23 de noviembre de 2001.

La nomenclatura utilizada por la Directiva 2013/40/UE, de 12 de agosto, refiriéndose a sistema de información y no a sistema informático es de todo punto incorrecta, ya que está haciendo alusión a una realidad más amplia que éste. El concepto de sistema de información, específicamente creado sobre la base de la teoría de la organización, tiene su sede en el tratamiento de información para

satisfacer las distintas necesidades de recursos humanos siendo su elemento fundamental el componente humano. No debe inducir a error el hecho de que hoy en día la mayor parte de los sistemas de información estén informatizados por razones de eficiencia con el hecho de que ambos conceptos se consideren equivalentes. El sistema informático puede formar parte del sistema de información o no, siendo que su integración en la estructura organizativa sea conveniente a efectos de cumplir con mayor corrección y celeridad su función.

En consecuencia, el concepto asumido por el artículo 197.1 bis es también erróneo, de tal forma que éste hubiera debido utilizar el de sistema informático. En cualquier caso, el concepto de sistema de información resulta incompatible con la pretensión de tutela pretendida por éste, motivo por el cual deberá ser interpretado restrictivamente conforme al contenido atribuido a aquel.

Por lo que respecta al sistema informático, éste se presenta así como un conjunto de capas y elementos jerárquicamente organizados sobre la base de una estratificación virtual, que empieza en el nivel más bajo en que consiste el hardware y que termina en un nivel alto de procesamiento de datos a través del software. Estos son los dos componentes que deben integrar todo sistema informático y de los cuales éste no puede prescindir. Desde esta perspectiva, sistema informático no debe entenderse como sinónimo de ordenador personal, sino que cualquier tipo de dispositivo que cumpla las características mencionadas queda amparado en la definición ofrecida. En consecuencia, el objeto material del delito de acceso ilícito es el sistema informático y como tal puede ser considerado cualquier dispositivo que esté dotado de dos elementos: software y hardware.

VI. Por lo que a los medios comisivos se refiere, el delito de acceso ilícito a un sistema informático previsto en el artículo 197.1 *bis* es un tipo de estructura cerrada que sólo puede cometerse de una forma: vulnerando las medidas de seguridad dispuestas para impedir el acceso. Esta afirmación contrasta en cierta medida con el tenor literal del precepto, que induce notablemente a confusión cuando comienza diciendo *[e]l que, por cualquier medio o procedimiento* en una incierta pretensión de amplitud e indeterminación por lo que se refiere a la forma de ejecución del hecho que acto seguido se restringe con la previsión de una modalidad específica de realización del tipo a unos medios comisivos determinados: *vulnerando las medidas de seguridad establecidas para impedirlo*. En cualquier caso, la expresión por cualquier medio o procedimiento debe ser interpretada en el sentido de que al amparo del precepto pueden ser castigados accesos realizados a través de las dos posibles vías que en la práctica existen para introducirse en un sistema informático:

> **a) Acceso físico:** el acceso a la localización espacial donde éste se encuentra y posterior acceso físico al sistema.
>
> **b) Acceso lógico:** el acceso remoto cometido a distancia desde otro sistema informático conectado a una red privada de área local o a una red pública global (Internet).

Estas dos formas de acceso sólo serán admisibles, no obstante, siempre y cuando dicho acceso se realice además vulnerando medidas de seguridad. En este sentido, la introducción de este elemento en la descripción típica tiene importantes consecuencias:

1. Para la aplicación del precepto, ya que actúa como un criterio de selección de la tutela penal al restringir los supuestos subsumibles en el mismo a los sistemas informáticos o telemáticos protegidos por medidas de seguridad, quedando fuera del ámbito típico todos aquellos que no dispongan de tales medidas. Esta limitación penal no es útil para cumplir su objetivo protector de un menoscabo de igual calibre pero substanciado por un procedimiento distinto. Debería, en consecuencia, castigarse también la conducta de quien accede al

sistema en contra de la voluntad del titular sin vulnerar ninguna medida de seguridad ofreciendo así una protección global a todos los ataques de la misma entidad sin discriminación alguna.

2. Para la determinación de la forma de ejecución del hecho, ya que pueden definirse distintos estándares de protección y, al amparo de ellos, realizar una interpretación más o menos restringida de este elemento típico. Aún así, puesto que la Ley no distingue, las medidas de seguridad deben interpretarse en un sentido amplio como todo dispositivo, medio, instrumento o mecanismo de protección del sistema, que tiene por finalidad la selección de los sujetos habilitados para acceder al sistema informático, excluyendo a terceros ajenos al mismo y también procurando la reserva del contenido. En este sentido, deben tener cabida tanto las medidas de carácter lógico como las de tipo físico y, dentro de éstas, tanto los instrumentos de hardware como los mecanismos de tipo organizativo ya estén dispuestos o no directamente sobre el sistema.

3. Por último, para la consumación del delito, siendo que la vulneración de las medidas de seguridad marcará el hito fundamental de ésta. Efectivamente, la lesión del bien jurídico se produce nada más sobrepasar las barreras de protección establecidas para impedirlo, momento en el que tiene lugar la perfección. El principal problema en este caso se plantea es el relativo a cuando se produce la efectiva vulneración de las medidas de seguridad, lo que dependerá de tres elementos: la presencia de éstas, su idoneidad y su superación.

a) La presencia de la medida hace referencia a la actualidad de la misma, ello en el sentido de que realmente exista algún medio de protección en el sistema, pero también en el de que éste encuentre activo en el momento en el que se produce el acceso. Así pues, debe excluirse la represión penal de la conducta en caso de desactivación o total ausencia de las medidas de seguridad.

b) La idoneidad objetiva de la medida permite restringir la concepción amplia de medidas de seguridad la que se ha hecho referencia a través del establecimiento de las condiciones que éstas deben reunir para ser consideradas válidas a los efectos de la aplicación del artículo 197 bis, condiciones cuya valoración se debe efectuar a través de criterios puramente objetivos, evitando que dependa de la concreta percepción del sujeto pasivo. A tal efecto, por idoneidad objetiva debe entenderse la vinculación directa entre la medida y el fin de exclusión pretendido. Esta vinculación se puede evaluar desde dos perspectivas: cualitativa y cuantitativa.

Desde un punto de vista cualitativo deben valorarse dos parámetros: por una parte, el grado de complejidad técnica que debe tener la medida, y, por otro, el nivel de eficacia que debe exigirse a la misma. En relación con la complejidad cabe decir que siempre que pueda establecerse dicha conexión directa entre la medida y el sistema, generalmente no debe exigirse al titular del sistema la disposición de especiales requerimientos de carácter técnico. En relación con la eficacia, igualmente no debe requerirse un determinado coeficiente sino únicamente que éstas tengan una eficiencia potencial para el fin pretendido. Además, desde el punto de vista de la eficacia, creo que las medidas de seguridad deben adecuadas a cada concreto sistema informático, de manera que la protección del sistema debe aumentar o disminuir en idéntica relación a la existencia de una mayor o menor conexión del sistema informático a las distintas posibilidades de red.

Desde un punto de vista cuantitativo, en general, la especial protección del sistema no debe apoyarse en la cantidad de obstáculos a superar por quien desee cometer la conducta típica, pues la existencia de una sola medida de seguridad puede ser idónea a los efectos de la culminación del

tipo. El criterio que regirá en este caso es el de la eficacia antes transcrito: se deberán superar todas aquellas que se hayan dispuesto específicamente para impedir esa concreta modalidad de acceso, lo que puede implicar la neutralización de una sola medida, de una parte de las varias dispuestas o de todas ellas, en función de la configuración de cada sistema informático.

c) En último lugar, la vulneración de las medidas de seguridad se produce cuando éstas son efectivamente superadas como consecuencia de la voluntad quebrantadora y anulatoria de quien accede ilícitamente al sistema. Ello no significa que deba producirse un menoscabo en el o los elementos de protección del sistema sino que es suficiente con su neutralización debiéndose entender ésta por en el sentido de superación o desactivación temporal.

VII. El artículo 197.1 *bis* contiene una referencia expresa no sólo a la parte positiva del tipo (que se ha estudiado en los capítulos precedentes), sino también a la parte negativa del tipo. De este modo, el tipo penal no se agota con los actos dirigidos al acceso o mantenimiento (desvalor de acción) y el menoscabo del bien jurídico —que se produce con la adquisición de la disponibilidad sobre el sistema y solo en el caso del acceso— (desvalor de resultado), sino que es necesario, además, que el sujeto activo no se halle autorizado para realizar dicho acceso (primer inciso) o que la permanencia en el sistema informático se realice en contra de la voluntad de quien tenga el legítimo derecho para excluirlo (segundo inciso). Ambos elementos deberán interpretarse de forma que se les atribuya idéntica significación.

De esta forma, el delito de acceso ilícito constituye una prohibición represiva con reserva de permiso en la que la autorización cumple la función de convertir en aprobada una conducta socialmente desaprobada como regla general: el acceso a un sistema informático ajeno. En consecuencia, este concepto es

expresión de la antijuricidad en tanto en cuanto si concurre autorización existirá afectación del bien jurídico seguridad informática y la conducta seguirá siendo jurídicamente relevante por no ser socialmente adecuada y normal, pero estará excepcionalmente autorizada por la ponderación que la autorización supone de otros intereses concurrentes en el caso concreto.

Por lo que al contenido de la autorización se refiere, la descripción típica exige que el autor acceda al sistema informático sin la autorización que sea debida. Esto significa que ésta debe ser válida jurídicamente, hecho que supone mantener la tipicidad de aquellos supuestos en los que existe una autorización oficial fáctica pero ésta no es plenamente válida en el plano jurídico. Así pues, en caso de que ésta no concurra el sujeto activo carece del título jurídico que legitima su acceso en ausencia clara e indudable de permiso suficiente tanto desde una perspectiva objetiva como subjetiva.

En consecuencia, el delito solo puede cometerse en aquellas situaciones en las que la autorización es necesaria, lo que implica afirmar la existencia de alguien con capacidad para autorizar en concreto el ejercicio del derecho de acceso. Esto implica fijar dos parámetros: quien puede autorizar y qué se puede autorizar.

Respondiendo a esta última pregunta, existirán tres supuestos de autorización: habilitación legal (*no permitido por el Derecho nacional*) y la autorización entendida como aquiescencia del titular del sistema (*no haya sido autorizado por el propietario u otro titular del derecho sobre el sistema o parte del mismo*) y la ya conocida en derecho español autorización oficial (administrativa o judicial).

Pasado ahora a determinar quien puede autorizar, debe afirmarse que tendrán esta capacidad todos sujetos titulares del sistema informático o con algún derecho sobre él que les atribuye la capacidad para poder autorizar válidamente el acceso. No obstante, teniendo en cuenta que pueden ser diversos los géneros de derechos que distintos sujetos ostentan sobre el sistema y que garantizan a sus titulares facultades suficientes para autorizar a un sujeto a acceder o

a utilizar legítimamente el sistema informático, cabe señalar que debe establecerse una prelación entre ellos cuando existen diversos derechos atendiéndose al título jurídico de cada uno de ellos y, si este es el mismo, dando prioridad a quien prohíbe.

VIII. De todo lo anterior se pueden extraer las siguientes propuestas de *lege ferenda*:

a) Trasladar el tipo penal al Título dedicado a la seguridad colectiva.

b) Eliminar la conducta de mantenimiento del tipo penal. Para dar una adecuada respuesta a este problema podría acudirse a la fórmula americana de *exceso de autorización*, que permitiría englobar no sólo las formas más graves de mantenimiento ilícito sino a todos aquellos supuestos en los que se ha concedido un determinado poder de autoridad sobre el equipo informático y éste ha sido sobrepasado.

c) Sustituir el concepto de sistema de información utilizado objeto material del delito por el de sistema informático.

d) Sustituir la expresión sin autorización por la de ilícitamente.

e) Si se optase por dejar la conducta de mantenimiento, el elemento relativo a las vulneración de las medidas de seguridad debería vincularse únicamente a la conducta de acceso.

f) Puesto que se ha concluido que existe afectación del bien jurídico seguridad informática en aquellos supuestos en los que el sistema no está dotado de medidas de seguridad, podría valorare la incriminación del acceso ilícito a un sistema informático sin ninguna protección debería como delito menor.

g) Finalmente, teniendo en cuenta que el hoy derogado artículo 197.3 cubría importantes lagunas de los dos

apartados que le precedían en el artículo 197 del Código penal, debería mantenerse en el sentido que se le ha dado en el presente estudio: como una cláusula de cierre de las afectaciones de la intimidad. Si bien, deberían castigarse sólo los casos más graves.

Con todo, se propone la siguiente redacción alternativa del precepto:

> *El que acceda o facilite el acceso ilícito a un sistema informático ajeno vulnerando las medidas de seguridad establecidas para impedirlo será castigado con la pena de prisión de seis meses a dos años.*
>
> *Se impondrá la pena inferior en grado si el acceso se produce en relación con un sistema que no dispone de tales medidas y que no tiene un carácter abierto.*

I. From a supranational perspective, the prevention, suppression and punishment of illegal access to a computer system has been a high-order issue for the different international organizations during the last three decades. In this sense, their main objective has been to achieve a full harmonization of the national legislation in the field of cybercrime, a matter wherein illegal access is the basic conduct of the common minimum standard above all the relevant offences.

The criminalization of illegal access to a computer system was already foresaw in the first text intended for that proposal, the report *Computer Related-Crime: Analysis of Legal Policy*, adopted in 1986 by the Organization for Economic Cooperation and Development. Moreover, the aim of punishing this behavior has been unvaryingly maintained over time, as is borne out by the fact of its inclusion between the bare minimum prohibitions in all the normative provisions —either with binding effect or only recommendatory in character— subsequently approved.

This need for protection is also reflected in the individual elements of the criminal prohibition, which haven't differed from its original configuration along the numerous provisions adopted within the different supranational organizations. In addition, the development of the criminalization has tended toward a more and more repressive protection, protection that has been only limited by the personal intention (malice) of the perpetrator

(recklessness is not admitted). Particularly, there are two (plus one) issues that have given rise to this expanded anti-crime measures:

a) On the one hand, considering that the mere unauthorized intrusion should in principle be illegal in itself and eliminating the requirement of additional protection to the system as an element of the crime, without any regard to whether they are protected or not or whether security devices are overcome. Originally, the infringement of security measures was considered an element of the crime in such a way as to exclude all the accesses to non protected computers. Soon thereafter, this requirement disappeared taking into consideration that the mere hacking affects the interests of organizations and individuals to manage, operate and control their systems in an undisturbed and uninhibited manner.

b) On the other hand, replacing the therm *unauthorized* with the expression *without right*. The reason for that was that the notion of *without right* is considered to be larger than the concept of *unauthorized*, which does not include all aspects of undesirable behavior, specifically the access infringing a law provision or the consent of the owner or any other right holder of the system or part of it.

c) Equally important would be the delineation of the access offence in relation to the system interception crime. Mere access does not imply neither a disruption of the system functions nor alteration or destruction of the system or its content. That's why both crimes, access and interception, initially linked to each other as a alternative mixt crime, came to be detached from each other.

The above statements are also applicable to the two texts with binding effect whereby the full legislative alignment in this area has culminated: the Council of Europe Convention on Cybercrime, signed in Budapest the 23 of November of 2001, and Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA. However, their content is specifically called for in some conclusions:

a) Illegal access to a computer system must be criminalized in all the member states of the European Union and the States Parties in the Convention on Cybercrime. The aim of this regulation is to establish or adopt the necessary guidelines in order to provide the minimum degree of harmonization required to achieve a legal cooperation to effectively punish this conduct.

b) For this purpose, both texts determine a minimum standard of criminalization of the crime. In this case, states are presented with two possibilities:

1. Many national legislations already contain provisions on illegal access offences, but their scope and constituent elements vary considerably. This states will have to revise their legislations in order to analyze if they are adapted to the text of the Cybercrime Convention and the Directive. In case they don't, they will have to modify their provisions to accomplish the supranational expectative.

2. Some States have not adopted any regulation criminalizing illegal access to computer system. This countries will have to approve new legislation in order to implement legal measures to prevent and deter this criminal behavior.

c) The Convention on Cybercrime allows the Parties to take the wide approach and criminalize mere hacking in accordance with the first sentence of Article 2, but, alternatively, Parties may attach any or all of the qualifying elements listed in the second part of the article. On the contrary, the Directive contains only one description: the punishment of illegal access to a computer system committed by the infringement of security measures. As can be seen in the preceding

sentence, the Directive contains a much more concrete approach than the Convention concerning the criminalization scope, covering a more specific number of cases. In this regard, it can be said that the Directive goes further than the Convention towards the harmonization objetive, preventing substantial variations between the national legislations.

d) Taking into account that the provisions of the Convention and the Directive are a bare minimum, States can extend the protection foresaw in the supranational norms.

II. At a state level, the national transposition of the mentioned provisions (Directive and Convention) has taken place within the majority of the member states from de European Union and the states parties on the Convention of Cybercrime.

Forty nine of the sixty five countries that are member of the European Union or parties of the Council of Europe and have ratified the Convention have approved legislation to criminalize illegal access to computer system. Only one member state of the European Union has not adopted any kind of regulation (Switzerland) and four of the members of Council of Europe have not subscribed on the Cybercrime Convention (Monaco, Russia, San Marino

and Ucrania). On the contrary, seven countries that are not member of the Council of Europe are party on it (Australia, Canada, Estados Unidos de América, Filipinas, Japón, Mauricio Islands and Dominic Republic).

From all of the countries stated above, only ten of them have also introduced the conduct of maintenance (Albania, Belgium, Canada, Spain, United States, France, Italy, Luxembourg, Moldavia and Turkey).

Referring to the material object, this was the major inconsistency of the reform in 2010. The Spanish Criminal Code adopted data as a material object, like another fifteen countries (Germany, Armenia, Australia, Austria, Bulgaria, Croacia, Greece, Island, Malta, Moldavia, Norway and Serbia) or three that directly mention information (Azerbaijan, Denmark and Slovakia. The rest of states mention the computer system (thirty three), information system as is mentioned in the Directive (Slovenia, Hungary, Lituania, Poland and Dominican Republic), or similar notions like automatized data system (France, Holland, Letonia, Luxembourg, Switzerland and Turkey) or merely computer (United States, Ireland, Japan, Mauricio Islands, Montenegro, Serbia, Sri Lanka, United Kingdom and the Republic of Macedonia) o computer service (Canada).

Concerning the different elements listed by the Convention, the Parties have only attached two to qualify the criminal offence:

a) On the one hand, the infringement of security measures, included by thirty three states (Albania, Germany, Andorra, Armenia, Australia, Austria, Azerbaijan, Bosnia and Herzegovina, Spain, Estonia, United States of América, Finland, Hungary, Italy, Japan, Letonia, Lituania, Montenegro, Norway, Poland, Serbia and Switzerland). Although, as was said before, this element was mandatory for the member states of the European Union, only seventeen have included it in the description of the criminal offence.

b) On the other hand, three countries (Moldavia, Reino Unido and Republic of Macedonia) have introduced the intention of obtaining data and only four have punished the conduct requiring the finality of causing harm (Slovakia, United Kingdom and Dominican Republic) or obtaining a benefit(Austria, Slovakia and Ireland).

III. The illegal access to a computer system was introduced as a criminal offence for the first time in the Spanish Criminal Code in 2010 and, subsequently, was amended in 2015 to fulfill a better

adaptation to the supranational regulation. This reform has achieved a more accurate the description of the crime.

Specifically, the conduct was introduced in the Spanish Criminal Code by the Organic Law 5/2010, of 22 June. This Law inserted the crime in the Title related to the crimes against intimacy, creating an equivalence to the two basic offences against this right and the new behavior. That was the reason why the Spanish legislator did not comply with the original configuration of the different elements of the crime and, instead of criminalizing illegal access to computer systems and protection the system, created a new offence that punished access of data. The material object of the crime was, in this sense, computer data.

In 2015, the conduct has been modified by the Organic Law 1/2015, of 30 of march, to create a separated and autonomous offence that, nevertheless was maintained in the same Title. However, it enables a better and more accurate interpretation of the law in favor of the aims sought by the Convention and the Directive.

In any case, both reforms constraints the structure of the next following conclusions as it was said in the different chapters of this text.

IV. The protected interest in the crime has varied according to the different configuration of the crime in the text introduced in 2010 and modified in 2015.

In 2010, taking into consideration that the crime was introduced as an equivalence offence in relation to the basic crimes against intimacy, the protected interest was, necessarily, the right to intimacy. In particular, three were the reasons for that: its systematic positioning among crimes against intimacy, its configuration as an equivalence offence to the basic crimes against this right and, finally, the fact that its scope of application was determined by a negative interpretation of the other two basic offences against intimacy mentioned before.

After the 2015 amendment, the illegal access has been maintained in the same Title but as a separated and autonomous offence. This fact allows for a new reinterpretation of the different elements of the crime and also a new forecast of the protected interest. In this sense, it is possible to state that the protected right in illegal access to computer system is, nowadays, the cyber or computer security.

The computer security must be presented as a new right of the citizens based on the need for protection from the individual and collective risks that arise from the new technologies in the Risk Society. In

this sense, this right can be identified also as a new criminal interest whose protection is completely justified by the need of safeguarding the managing, operation and controlling of computer systems in an undisturbed and uninhibited manner as a way to avoid the commission of more dangerous forms of computer-related offences.

From this perspective, illegal access to computer system covers the basic offence of dangerous threats to and attacks against the security of computer systems in a short term and the anticipation of the criminal protection in relation to all those other possible crimes in a long term. This leads to the consideration of the offence as a crime of damage-endangerment, that harms a supraindividual interest, the computer security, and endangers many other supraindividual and individual rights. This supraindividual nature gives rise to the idea that it should have been criminalized among crimes against collective security.

The right to computer security is perfectly embeddable in the article 18.4 of the Spanish Constitution, that recognizes the right of the citizens to fully exercise their rights in a undisturbed and uninhibited manner regarding to the use of technology.

Its content can be seen from a positive and negative point of view:

a) Positive perspective: a right to a satisfactory use of IT.

b) Negative perspective: a right of not be attacked in the exercising of the right mentioned above.

V. In the Spanish Criminal Code, the illegal access to computer system has been configured alternatively to another behavior: the maintenance in the computer system without authorization.

1. The first conduct punishes to access or giving access to a computer system. As can be noticed, all kind of criminal involvement in the commission of the crime is considered perpetration since 2015, so criminal participation (the act of giving access) is counted as perpetration.

Access comprises an electronic intrusion in a computer system of another person or enterprise without causing any interference or disruption on its functioning nor acknowledging, damaging or obtaining its content.

There are two ways in which the illegal access can be perpetrated: first, the physical intrusion and remote intrusion to a computer, and second, the entering of the whole or any part of a computer system.

The completion of the crimen takes place when the perpetrator acquires the availability of the computer system. This availability consists of a situation where the perpetrator has the condition of accessing or obtaining the data or any other information stored on the computer. Therefore, this status constitutes the result of the crime, result that occurs instantly after getting the availability.

Another condition is required to fulfill the completion: the infringement of security measures. The perpetrator has to break all the protection devices that hamper the acquisition of that availability. If he doesn't reach this status the conduct will be punished as an attempt.

2. The second alternative criminalizes the maintenance of the perpetrator in the computer system produced after a legal access or, better said, the mere ilegal use of it. Specifically this part of the crime covers four forms of crime: the temporary or modal abuse of the computer, the mere use of the computer after withdrawal of consent, the malice use of the

computer produced after a involuntary or casual access and the cases of exceptional access.

This criminal behavior consists merely in a permanent and conduct crime, which consummation doesn't require the infringement of security measures. This element, consequently, is only linked to the first form of the crime (access).

In any case, the mere maintenance should not have been criminalized as a status crime according to the principle of *ultima ratio* and the harm principle. Its harmfulness is not sufficiently relevant and therefore judges should moderate its application excluding all the cases where there exists only a remote affectation of the computer security (principle of insignificance).

VI. As indicated before, the main change introduced in 2015 was regarded to the material object of the crime, that has now become the information system instead of computer data.

1. In 2010, the crime was introduced in the paragraph .3 of the article 197, as an equivalent offence to the two basic crimes against intimacy, punished in the article 197.1 and .2 of the Spanish Criminal Code. In order to adapt the conduct to this kind of crimes, the legislator modified the original elements of the illegal access, so that the crimes as material object was

conformed by the data contained in a computer system. But this features could be also predicated of the material objects stowed in the two paragraphs mentioned above, so, in the end, its scope of application was determined by a negative interpretation of the other two basic offences against intimacy mentioned before: the new paragraph led to a norm concurrence that had to be solved by the application of first criterion in article 8 of the Spanish Criminal Code, the principle of speciality.

In the end, the scope of application of the article 197.3 was:

a) Access without procuration.

b) Access to data contained in a computer system that concern to another person than owner of the computer.

c) Access to non reserved data.

d) Access to data contained in a computer system but not registered in a data basis.

e) Access to non personal of familiar data.

From a positive perspective, could be fully the definition of computer data under the Convention and

the Directive: any representation of facts, information or concepts in a form suitable for processing in a computer system, including a program suitable to cause a computer system to perform a function.

2. After 2015, the material object of the crime is the information system, a notion with a very broad sense that goes even further than the concept of computer system. This modification, that follows the text of the Directive, matches of course much better with the purpose of the supranational provision, but extends uncertainly its scope of application. The notion of information system is indeed much more indeterminated than the notion of computer system because it consists essentially in a business concept based on the theory of organization and efficiency within enterprises that includes the personal factor as the main vector of getting results.

In any case, the concept of information system is defined in the Directive by using the same meaning than the notion of computer system contained in the Convention, so that, in the end, both terms must be considered synonyms. In this sense, computer system will be any device consisting of hardware and software developed for automatic processing of digital data. It may include input, output, and storage facilities.

VI. In the Spanish Criminal code, illegal access to a computer system necessarily requires the infringement of security measures.

Although the description of the crime begins with the phrase: *who following any procedure*, thereupon the criminal code restricts the punishment of the offence to the computer systems which include protection tools installed. That expression must be interpreted in the sense of applying the crime to physical intrusions as well as remote ones.

Regarding to the security measures, the introduction of this element has specifically three consequences:

1. First of all, it excludes the protection of the computer systems without security measures installed.

2. In the second place, it forces to define a standard of security and to fix criteria to delineate the nature and features that will be accepted as a security measures. In this sense, security measure must be understood in a very broad sense as any device, media or instrument used to protect the computer system and exclude others from it. Consequently, the scope of application will include not only logical measures but also physical devices or methods.

3. Finally, the requirement of this element affects to the consummation of the crime, because it will not be completed until the perpetrator infringes the security measures and gets availability over the computer system. The infringement is, for this purpose, a condition to get availability. This requires:

a) Activation: the security measure must be activated during the commission of the crime.

b) Suitability: the measure must be suitable for the protection of the computer system according to the type of intrusion. The computer will have to be protected with logical measures if it is connected to a network or will need physical measures if it is not. In any case, a special grade of complexity or efficiency related to the measure (qualitative suitability) or a concrete number of measures (quantitative suitability) should not be required.

VII. The act must also be committed without authorization.

In addition to the explanation given above on this expression, it means that there is no criminalisation of the access authorized by a Law, an oficial way or by the owner or other right holder of the system or part of it. And only when it is legally

needed. Moreover, there is no criminalisation for accessing a computer system that permits free and open access by the public, as such access is with right.

This element expresses antijuridicity and must be interpreted in the sense of the expression without right contained in the Convention and the Directive.

BIBLIOGRAFÍA

BIBLIOGRAFIA

NOTA: DEBE TENERSE EN CUENTA QUE EN EL PRESENTE ESTUDIO SE HA TRABAJADO SOBRE LA BASE DE DOS VERSIONES DISTINTAS DEL TEXTO DEL CÓDIGO PENAL, LA VIGENTE ENTRE LOS AÑOS 2010 Y 2015 Y LA VIGENTE DESDE 2015 HASTA LA ACTUALIDAD. POR ESTE MOTIVO, LA BIBLIOGRAFÍA ESPAÑOLA BÁSICA HA SIDO UTILIZADA Y CITADA RESPETANDO ESTA DUALIDAD: SE HAN EMPLEADO MANUALES SOBRE LEGISLACIÓN HOY DEROGADA PARA COMENTAR EL TEXTO VIGENTE DESDE 2010 A 2015 Y TAMBIÉN SE HAN UTILIZADO LAS TODAVÍA ESCASAS REFERENCIAS PUBLICADOS TRAS LA REFORMA PARA APOYAR LAS IDEAS PLASMADAS SOBRE ÉSTA.

ACALE SÁNCHEZ, M. 2002. Los delitos de mera actividad. *Revista de derecho Penal y Criminología,* nº 10**,** 11 - 45.

ALBRECHT, P.-A. 2000. El Derecho penal en la intervención de la política populista. *La insostenible situación del Derecho penal (ROMEO CASABONA, C. M. (dir.)).* Granada: Comares.

ALDAMA BAQUEDANO, C. 1993. Los medios informáticos. *Poder Judicial,* nº 30**,** 9-26.

ALEGRE MARTÍNEZ, M. Á. 1997. El derecho a la propia imagen, Madrid, Tecnos.

ALEO, S. y PICA, G. 2012. Diritto penale. Parte speciale II, CEDAM.

ALIBRANDI, L. 2011. Codice Penale. Aggiornato con tutte le ultime novità normative e guirisprudenziali, Piacenza, Casa Editrice La Tribuna.

ALMA, M. y PERRONI, C. 1997. Riflessioni sull'attuazione delle norme a tutela dei sistemi informatici. *Diritto penale e proceso,* 71.

ALONSO DE ESCAMILLA, A. 2013. Tema 10. Delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del

domicilio. *Delitos y Faltas. La Parte Especial del Derecho penal*. Madrid: Colex.

ALTENHAIN, K. y WIETZ, C. 2013. § 202a. Strafgesetzbuch Kommentar (MATT, HOLGER y RENZIMOWSKI, JOACHIM) MÜNCHEN: C.H.B BECK.

ALTÉS TÁRREGA, J. A. 2002. El acoso sexual en el trabajo, Valencia, Tirant lo Blanch.

ALVAREZ GARCÍA, F. J. 1991. Bien jurídico y Constitución. *Cuadernos de política criminal*, 5-44.

ÁLVAREZ VIZCAYA 2002. Consideraciones político criminales sobre la delincuencia informática: el papel del Derecho penal en la red. *Cuadernos de derecho judicial*.

AMAYA AMAYA, J. 2010. Sistemas de información gerenciales, ECOE Ediciones.

AMORE, S., STANCA, V. y STARO, S. 2006. I crimini informatici. Doctrina, giurisprudenza ed aspetti tecnici delle investigazioni, Matelica, Halley Editrice SRL.

ANARTE BORRALLO, E. 2001a. Consideraciones sobre los delitos de descubrimiento de secretos (I) En especial, el art. 197.1 del Código Penal. *Jueces para la democracia,* 43**,** 50-61.

ANARTE BORRALLO, E. 2001b. Impactos de las nuevas tecnologías en el sistema penal: aproximación al derecho penal en la sociedad de la información. *Derecho y conocimiento: anuario jurídico sobre la sociedad de la información y del conocimiento***,** 191-260.

ANARTE BORRALLO, E. y DOVAL PAÍS, A. 2012. Límites de la ley penal a propósito del nuevo delito de intrusión informática. *Revista General de Derecho Penal*.

ANARTE BORRALLO, E. y DOVAL PAÍS, A. 2015. Lección XIX. Delitos contra a la intimidad, el derecho a la propia imagen y la

inviolabilidad del domicilio (1). Delitos de descubrimiento y revelación de secretos. Derecho penal: Parte Especial (BOIX REIG, JAVIER (dir.)). Madrid: Iustel.

ANDREU, R., RICART, J. R. y VALOR, J. 1996. Estrategia y sistemas de información (2ª Edición), Madrid, MC Graw-Hill.

ANTOLISEI, F. 2008. Manuale Diritto penale Parte Speciale I, Milano, Giuffrè Editore.

ANTÓN ONECA. 1986. Derecho penal 2ª Edición, Madrid: Akal.

APARICIO SALOM, J. 2009. Estudio sobre la Ley Orgánica de Protección de Datos de Carácter Personal, Navarra, Aranzadi.

ASOCIACIÓN INTERNACIONAL DE DERECHO PENAL 1992. Recomendaciones sobre infracciones informáticas y otros delitos contra la tecnología informática. *Revue Internationale de Droit Penal*, 64.

ASOCIACIÓN INTERNACIONAL DE DERECHO PENAL 1995. Recomendaciones sobre infracciones informáticas y otros delitos contra la tecnología informática. *Revue Internationale de Droit Penal*, 66.

ATERNO, S. 2000. Sull'accesso abusivo a un sistema informatico o telematico, Cassazione Penale.

AZURMENDI ADARRAGA, A. 1997. El derecho a la propia imagen: su identidad y aproximación al derecho a la información, Madrid, Civitas.

BACIGALUPO ZAPATER, E. 2002. Documentos electrónicos y delitos de falsedad documental. *Revista Electrónica de Ciencia Penal y Criminología*, nº 14.

BALLESTER CARDELL, M. 1998. La intimidad como fundamento de la inviolabilidad del domicilio, Palma, Universitat de les Illes Balears.

BEQUAI, A. 1990. Recomendation (89) 9 on computer related-crime. Report by the European Committee in Crime Problems, Strasbourg, Council of Europe.

BEM, M. A. 2010. L'intrusion et les atteintes aux systemes informatiques sanctionnees par le Droit Penal.

BERENGHELLA, F. y BLAIOTTA, R. 1995. Diritto penale dell'informatica e beni giuridici. *Cassatione penale*.

BLAIOTTA, R. 1999. Le fattispecie penali introdotte dalla legge sulla privacy. *Cassatione penale*, 5.

BLAIOTTA, R. 2002. Le modifiche alle fattispecie penali previste dalla legge sulla protezione dei dati personali. *Cassatione penale*, 9.

BLASCO GASCÓ, F. D. P. 2007. Patrimonialidad y personalidad de la imagen, Barcelona, Bosch.

BLASCO GASCÓ, F. D. P. 2008. Algunas cuestiones del derecho a la propia imagen. Bienes de la personalidad. XIII Jornadas de la Asociación de Profesores de Derecho civil. Murcia: Edit.um.

BOIX REIG, F. J. 1989. Protección jurídico-penal de la intimidad e informática. *Poder Judicial***,** 17-38.

BOLEA BARDÓN. 2011. Título X. Delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio en Comentarios al Código penal (CORCOY BIDASOLO, M. y MIR PUIG, S. (dir.)), Valencia: Tirant lo Blanch, 2011.

BONILLA SÁNCHEZ, J. J. 2010. Personas y derechos de la personalidad, Madrid, Reus.

BORJA JIMÉNEZ, E. 1990. *El delito de allanamiento de morada,* Universidad de Valencia, Tesis doctoral inédita.

BORJA JIMÉNEZ, E. 1997. El bien jurídico protegido en el delito de allanamiento de morada. *Estudios juridicos en memoria del profesor Dr. D. José Ramón Casabó Ruiz.* Valencia: Universitat de València.

BORKO, H. 1965. Information Science: What is it? *Amercian Documentation,* 19, 1, 3-5.

BORRUSO, R. 1994a. La tutela del documento e dei dati. *Profilli penali dell'informatica* Milano: Giufrrè Editore.

BORRUSO, R., BUONOMO, G., CORASANITI, G. y D'AIETTI, G. 1994. *Profilli penali dell'informatica,* Milano, Giufrrè Editore.

BOSCH, N. 2014. § 202a. Strafgesetzbuch Kommentar (SATZGER, HELMUT; SCHLUCKBIER, WILHELM y WIDMAIER, GUNTER), 2. Auflage. Köln: Carl Heymanns Verlag.

BRAGHÒ, G. 2008. Delitto di accesso abusivo a sistema informatico o telematico. *Diritto dell'Internet*.

BRANDEIS, L. y WARREN, S. 1890. The right to privacy. *Harvard Law Review* [Online], vol. IV, nº 5. Available: http://groups.csail.mit.edu/mac/classes/6.805/articles/privacy/Privacy_brand_warr2.html.

BÜHLER, C. 1987. Ein Versuch, Computerkriminellen das Handwerk su legen: Das Zweite Gesetz zur Bekämpfung der Wirtschaftskriminalität. *Monatsschrift für Deutsches Recht*.

BUSTOS RAMÍREZ, J. 1986. Los bienes jurídicos colectivos (Repercusiones de la labor legislativa de Jiménez de Asúa en el Código penal de 1932). *Revista de la Facultad de Derecho de la Universidad Complutense,* nº 11.

BUSTOS RAMÍREZ, J. 1987. Control social y sistema penal, Barcelona, PPU.

BUSTOS RAMÍREZ, J. 1991. Derecho penal. Parte Especial, Barcelona, Ariel.

CABALLERO BRUN, F. 2008. *Insolvencias punibles,* Madrid, Iustel.

CADOPPI, A., CANESTRARI, S., MANNA, A. y PAPA, M. 2011. Trattato di Diritto penale. Parte Speciale - IX Il delitti contro la libertà sessuale, la libertà morale, l'inviolabilità del domicilio e l'inviolabilità dei segreti, Torino, UTET Giuridica.

CALDERÓN, Á. y CHOCLÁN MONTALVO, J. A. 1999. *Derecho penal. Parte Especial II,* Barcelona, Deusto.

CANCIO MELIÁ. 1998. Conducta de la víctima e imputación objetiva en derecho penal: estudio sobre los ámbitos de responsabilidad de víctima y autor en actividades arriesgadas, J. M. Bosch Edito.

CANNATA, S. 2006. Parte II. I delitti contro la riservatezza informatica e telamatica del domicilio. *I reati contro la persona. II. Reati contro l'onore e la libertà individuale (Papa, Michele (dir.)).* Torino: UTET.

CARBONELL MATEU, J. C. 1994. Breves reflexiones sobre la tutela de los llamados intereses difusos. *Cuadernos de derecho judicial,* XXXVI.

CARBONELL MATEU, J. C. y GONZÁLEZ CUSSAC, J. L. 2010. Delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio. *Derecho penal. Parte especial.* Valencia: Tirant lo Blanch.

CARBONNIER, J. 1963. Flexible droit. Pour une sociologie du droit sans rigueur, Paris, Sirey.

CARBONNIER, J. 1974. Derecho Flexible. Para una sociología no rigurosa del Derecho (traducción Luís Díez-Picazo y Gullón, Madrid, Tecnos.

CARINGELLA, F., MAZZAMUTO, S. y MORBIDELLI, G. 2010. *Manuale di Diritto penale. Parte speciale,* Roma, DIKE.

CARMONA SALGADO, C. 1996. La intimidad como bien jurídico protegido, a proósito de la reforma penal sobre secreto de las telecomunicaciones, de 23 de diciembre de 1994, Tomo XVII. *Comentarios a la Legislación Penal (COBO DEL ROSAL (dir.) BAJO FERNÁNDEZ (coord.).* Madrid: EDERSA.

CARRASCO ANDRINO, M. D. M. 2010a. El delito de acceso ilícito a los sistemas informáticos. Comentarios a la Reforma Penal de 2010 (ÁLVAREZ GARCÍA, FRANCISCO JAVIER y GONÁLEZ CUSSAC, JOSÉ LUÍS (dir.)). Valencia: Tirant lo Blanch.

CARRASCO ANDRINO, M. D. M. 2010b. El delito de acceso ilícito a los sistemas informáticos. La adecuación del Derecho penal español al ordenamiento de la Unión Europea. La política criminal europea. Tirant lo Blanch.

CARRASCO ANDRINO, M. D. M. 2011. Lección 23ª Descubrimiento y revelación de secretos. *Derecho penal español. Parte especial II (ÁLVAREZ GARCÍA, FRANCISCO JAVIER).* Valencia: Tirant lo Blanch.

CASAS BARQUERO. 1987. El Consentimiento en el derecho penal, Córdoba: Instituto de Criminologıa de la Universidad Complutense.

CASTELLI, G. M. 1986. *Il dolo informatico,* Milano, Franco Angeli.

CASTELLÓ NICAS, N. 2000. El concurso de normas penales, Granada, Comares.

CASTILLA BAREA, M. 2011. Las intromisiones legítimas en el derecho a la propia imagen, Navarra, Thomson Reuters.

CASTIÑEIRA PALOU, M. T. 2011. Tema 7. Delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio. *Lecciones de Derecho penal.* Barcelona: Atelier.

CASTIÑEIRA PALOU, M. T. y ESTRADA CUADRAS, A. 2015. Delitos contra la intimidad, el derecho a la propia imagen y la

inviolabilidad del domicilio. Lecciones de derecho penal: Parte especial (SILVA SÁNCHEZ, JESÚS MARÍA (dir.) y RAGUÉS VALLÉS, RAMÓN (coord.)). Barcelona: Atelier.

CATULLO, F. G. 2006. Il caso Vierika: un interessante pronuncia in materia di virus informatici e prova penale digitale. I profili sostanziali. *Diritto dell'Internet*.

CECCACCI, G. 1994. *Computer crimes,* Milano, Edizioni FAG.

CEREZO MIR. 1982. El delito como acción típica, evolución del concepto dogmático del tipo, en Estudios penales. Libro Homenaje al Profesor Antón Oneca (Salamanca: Universidad de Salamanca.

CEREZO MIR. 1989. El consentimiento como causa de exclusión del tipo y como causa de justificación, en Estudios de derecho penal y criminología: en homenaje al profesor José María Rodríguez Devesa, Madrid: Facultad de Derecho:Universidad Nacional de Educación a Distancia, 1989.

CEREZO MIR. 2002. Curso de Derecho penal español. Parte General. Tomo II. Teoría jurídica del delito, Madrid: Tecnos.

CERQUA, L. D. 2000. Accesso abusivo e frode informatica: l'orientamento della Cassazione. *Diritto e pratica delle società*, nº 16.

CHOCLÁN MONTALVO, J. A. 2006. Infracciones patrimoniales en los procesos de transferencia de datos. *El cibercrimen: nuevos retos jurídico-penales, nuevas respuestas político-criminales.* Comares.

CIRCULAR DE LA FISCALÍA GENERAL DEL ESTADO Circular de la Fiscalía General del Estado, número 2/1989, de 20 de abril, Precisiones conceptuales sobre algunos aspectos de la formulación típica y de la responsabilidad en los delitos contra la propiedad intelectual tras la Ley Orgánica 6/1987, de 11 de noviembre.

COBO DEL ROSAL, M. 1971. Sobre el apoderamiento documental para descubrir los secretos de otro (párrafo segundo del artículo 497

del Código penal. *Anuario de Derecho Penal y Ciencias Penales*, Tomo XXIV Fascículo III.

COBO DEL ROSAL, M. y ZABALA LÓPEZ-GÓMEZ, C. 2006. *El acoso sexual*, Madrid, CESEJ EDICIONES.

CODINA BONILLA, L. 1996. La investigación en sistemas de información. Actas del Seminario: Tendencias de investigación en Documentación (TRAMULLAS SAZ, JESÚS (dir.)). Zaragoza: Servicio de Publicaciones. Universidad Zaragoza.

COLÁS TURÉGANO, M. A. 2013. La importancia del consentimiento del sujeto pasivo en la protección penal del derecho a la propia imagen: a propósito de la propuesta de modificación del art. 197 CP anteproyecto de octubre de 2012. Revista Boliviana de Derecho, 160-179.

COLÁS TURÉGANO, M. A. 2015. Nuevas conductas delictivas contra la intimidad, en Comentarios a la reforma penal de 2015 (GONZÁLEZ CUSSAC, J. L.), Valencia: Tirant lo Blanch.

COLÁS TURÉGANO, M. A. 2016. El delito de intrusismo informático tras la reforma del Código penal español de 2015. Revista Boliviana de Derecho, 21, 210-229.

CONGRESO DE LOS DIPUTADOS: Iniciativa de Proyecto de Ley, 2013.

CONGRESO DE LOS DIPUTADOS: Emmiendas e índice de enmiendas. Documento 121/000065, 2014.

CONGRESO DE LOS DIPUTADOS: Informe de la Ponencia, 2015.

CORCOY BIDASOLO, M. 1999. Delitos de peligro y protección de bienes jurídico-penales supraindividuales, Valencia, Tirant lo Blanch.

CORCOY BIDASOLO, M. 2007. Problemática de la persecución penal de los denominados delitos informáticos. *Eguzkilore: Cuaderno del Instituto Vasco de Criminología,* nº 21.

CORRERA, M. y MARTUCCI, P. P. 1986. I reati commessi con l'uso del computer. Banche dei dati e tutela della persona, Padova, CEDAM.

CORRIAS LUCENTE, G. 2001. Brevi note in tema di accesso abusivo e frode informatica: uno strumento per la tutela penale dei servizi. *Diritto dell'informazione e dell'informatica*, nº 17.

CORRIPIO GIL-DELGADO, M. D. L. R. y MARROIG POL, L. 2001. El tratamiento de los datos de carácter personal y la protección de la intimidad en el sector de las telecomunicaciones, Madrid, Agencia de Protección de datos.

COUNCIL OF EUROPE. 2001. Explanatory Report to the Convention on Cybercrime. Available: http://conventions.coe.int/treaty/en/reports/html/185.htm.

COUNCIL OF EUROPE. 2012a. T-CY Guidance Note #1 On the notion of "computer system". Article 1.a Budapest Convention on Cybercrime. Available: www.coe.ent/TCY.

COUNCIL OF EUROPE. 2012b. T-CY Guidance Note #6 Crititcal information infraestructure attacks. Available: www.coe.ent/TCY.

CRESPI, A., FORTI, G. y ZUCCALÀ, G. 2011. *Comentario breve al Codice Penale,* Padova, CEDAM.

CUESTA PASTOR, P. J. 2002. Delitos obstáculo: tensión entre política criminal y teoría del bien jurídico, Comares.

CUOMO, L. 2000. La tutela penale del domicilio informatico. *Cassatione penale*, nº 11.

CUOMO, L. y IZZI, B. 2002. Misure di sicurezza e accesso abusivo ad un sistema informatico o telematico. *Cassatione penale*.

CUOMO, L. y RAZZANTE, R. 2009. La nuova disciplina dei reati informatici, Torino, Giappchelli Editore.

D'AIETTI, G. 1994. La tutela del documento e dei dati. *Profilli penali dell'informatica.* Milano: Giufrrè Editore.

D'ARCANGELO, C. 2006. Accesso abusivo ad un sistema informatico mediante induzione in errore dell'utente. *Il Corriere del Merito*.

D'ARCANGELO, C. 2008. L'accesso abusivo ad un sistema informatico nell'era di Internet. *Il Corriere del Merito*.

DAVARA RODRÍGUEZ, M. A. 2003. La protección de datos personales en el sector de las comunicaciones electrónicas, Madrid, Univerdidad Pontificia Comillas.

DAVARA RODRÍGUEZ, M. A. 2007. Manual de Derecho informático, Navarra, Aranzadi.

DE DOMINGO, T. 2001. *¿Conflictos entre derechos fundamentales?*, Madrid, Centro de Estudios Políticos y Constitucionales.

DE LA CUESTA ARZAMENDI, J. L. y PÉREZ MACHÍO, A. I. 2010. Ciberdelincuentes y cibercíctimas. *Derecho penal informático.* Navarra: Thomson Reuters.

DE LA GANDARA VALLEJO. 1995. Consentimiento, bien jurídico e imputación objetica, Madrid: Colex.

DE LA MATA BARRANCO, I. y DE LA MATA BARRANCO, N. J. 2004. La figura de la autorización en la lesión de bienes jurídico-penales de carácter supraindividual. *Dogmática y ley penal. Libro homenaje a Enrique Bacigalupo.*

DE LA MATA BARRANCO. 1997. El consentimiento presunto ante comportamientos realizados en interés propio, en Política criminal y nuevo derecho penal: Libro homenaje a Claus Roxin, Barcelona: Bosch

DE LA MATA BARRANCO, N. 2007. Los delitos vinculados a las nuevas tecnologías de la información y la comunicación en el Código penal español. *Cuadernos penales José María Lidón*, nº 4**,** 41-84.

DE LA MATA BARRANCO, N. y HERNÁNDEZ DÍAZ, L. 2010. Los delitos vinculados a la informática en el Derecho penal español. *Derecho penal informático (DE LA CUESTA ARZAMENDI, JOSÉ LUÍS (dir.) y DE LA MATA BARRANCO, NORBERTO (coord.)).* Navarra: Thomson-Reuters.

DE LA MATA BARRANCO, N. J. 2010a. Ilícitos vinculados al ámbito informático: La respuesta penal. *Derecho penal informático.* Navarra: Thomson Reuters.

DE LA MATA BARRANCO, N. J. 2010b. Los delitos vinculados a la informática en el Derecho penal español. *Derecho penal informático.* Navarra: Thomson Reuters.

DE NOVA LABIÁN, A. J. D. 2010. Delitos contra la Propiedad Intelectual en el ámbito de Internet., Dykinson.

DE PABLOS HEREDEROS, C. 2004. Informática y comunicaciones en la empresa, Madrid, ESCIC.

DE SANZO, F., D'ALFONSO, E., NOTARO, A., SANTOMASSIMO, G. y QUARANTA, V. 2009. Giurisprudenza penale: Reati di Parte Speciale del Codigo Penale e delle principali leggi complementari (FAVA, PASQUALE (dir.)), Dogana, Maggioli.

DE URBANO CASTRILLO, E. 2011. El derecho al secreto de las comunicaciones, Madrid, La Ley.

DE VEGA RUIZ, J. A. 1991. El acoso sexual como delito autónomo, Madrid, COLEX.

DE VERDA Y BEAMONTE, J. R. 2007. Veinticinco años de Aplicación de la Ley Orgánica 1/1982, de 5 de mayo, de Protección Civil del

Derecho al Honor, a la Intimidad Personal y Familiar y a la Propia Imagen, Navarra, Thomson Aranzadi.

DE VERDA Y BEAMONTE, J. R. 2011. El derecho a la imagen desde todos los puntos de vista. *Revista Aranzadi de Derecho y Nuevas Tecnologías,* nº 9.

DELPINO, L. 2003. *Diritto penale. Parte Speciale,* Napoli, Gruppo Editoriale Esselibri - Simoni.

DESTITO, V. S., DEZZANI, G. y SANTORIELLO, C. 2007. *Il Diritto penale delle nuove tecnologie,* Padova, CEDAM.

DEUTSCHER BUNDESTAG 1986. Drucksache 10/5058, Entwurf eines Zweiten Gesetzes zur Bekämpfung der Wi rtschaftskriminalität (2. WiKG).

DEUTSCHER BUNDESTAG 2006. Drucksache 16/3656, Entwurf eines ... Strafrechtsänderungsgesetzes zur Bekämpfung der Computerkriminalität (... StrÄndG).

DI GIANNANTONIO, E. 1997. Manuale di diritto dell'informatica, Padova, CEDAM.

DI GIANNANTONIO, E. 2001. L'oggeto giuridico dei reati informatici. *Cassatione penale*.

DI LEMBO 2005. L'acceso abusivo ad un sistema informatico. *Rivista penale*.

DI PUNZIO, I. y NATALINI, A. 2006. Manuale completo di diritto penale. Parte Generale. Parte Speciale, Dogana, Maggioli Editore.

DIETRICH, R. 2009. Dietrich Das Erfordernis der besonderen Sicherung im StGB am Beispiel des Ausspähens von Daten, § 202a StGB, Berlin, Duncker & Humblot GmbH.

DIETRICH, R. 2011. Die Rechtsschutzbegrenzung auf besonders gesicherte Daten des § 202a StGB. *Neue Zeitschrift für Strafrecht*, 247 - 254.

DÍEZ RIPOLLÉS, J. L. 1997. El bien jurídico protegido en un Derecho penal garantista. *Jueces para la democracia,* 30.

DIN 1988. DIN 44300 Bbl 1: Informationsverarbeitung; Begriffe, Alphabetisches Gesamtverzeichnis, Beuth Verlag, Deutsches Institut für Normung.

DOLCINI, E. y MARINUCCI, G. 2011. *Codice penale commentato,* Milano, IPSOA.

DOPICO GÓMEZ-ALLER, J. 2004. "Comisión por omisión y principio de legalidad. El artículo 11 CP como cláusula interpretativa auténtica". *Revista de derecho penal y criminología*, 279-316.

DOVAL PAÍS, A. 2000. La intimidad y los secretos de empresa como objetos de ataque por medios informáticos. *Eguzkilore: Cuaderno del Instituto Vasco de Criminología,* 22, 89-115.

DOVAL PAÍS, A. y JAREÑO LEAL, A. 2000. Revelación de datos personales, intimidad e informática (Comentario a la STS 234/1999 de 18 de febrero). *La Ley: Revista jurídica española de doctrina, jurisprudencia y bibliografía,* 4, 1672-1680.

DOVAL PAÍS, A. y JAREÑO LEAL, A. 2001. Revelación de datos personales, intimidad e informática (Comentario a la STS 234/1999 de 18 de febrero). El Nuevo Derecho Penal Español. Estudios Penales en Memoria del Profesor José Manuel Valle Muñiz (QUINTERO OLIVARES, GONZALO (dir.) y MORALES PRATS (coord.)). Pamplona: Aranzadi.

DOYLE, C. 2014. Cybercrime: A Sketch of 18 U.S.C. 1030 and Related Federal Criminal Laws. *Congressional Research Service*.

DOYLE, C. y BARLETT WEIR, A. 2006. Cybercrime An Overview of the Federal Computer Fraud and Abuse Statute and Related Federal Criminal Laws, New York, Novinka Books.

DURHAM, C. 1992. The Emerging Structures of Criminal Information Law: Tracing the Contours of a New Paradigm. *Revue Internationale de Droit Penal,* 64.

ELVIRA PERALES, A. 2007. Derecho al secreto de las comunicaciones, Madrid, Iustel.

ERNST, S. 2007. Das neue Computerstrafrecht. *Neue Juristische Wochenschrift,* 37**,** 2661 - 2666.

ERNST, S., GRZEBIELA, T., MANKOWSKI, P., PIERROT, O., REICHENBACH, M., SCHORR, M. y SCHULTIS, K. 2004. *Hacker, Cracker & Computerviren: Recht und Praxis der Informationssicherheit,* Köln, Schmidt, Otto.

ESCUCHURI AISA, E. 2004. Teoría del concurso de leyes y de delitos: bases para una revisión crítica, Comares.

ESCUDERO GARCÍA-CALDERÓN. 2014. El consentimiento en Derecho penal, Valencia: Tirant lo Blanch.

ESTADELLA YUSTE, O. 1995. La protección de la intimidad frente a la transmisión internacional de datos personales, Madrid, Tecnos.

EUROPEAN UNION COMISSION 2001. Creating a Safer Information Society by Improving the Security of Information Infraestructures and Combating Computer-related Crime.

EUROPEAN UNION COMMISSION. 2001. Network and Information Security: Proposal for A European Policy Approach. Available: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2001:0298:FIN:ES:PDF.

FARALDO CABANA, P. 2010a. De la usurpación de funciones públicas y el intrusismo. *Comentarios al Código penal (GÓMEZ TOMILLO, M. (dir.)).* Valladolid: Lex Nova.

FARALDO CABANA, P. 2010b. De las insolvencias punibles. *Comentarios al Código penal (GÓMEZ TOMILLO, M. (dir.)).* Valladolid: Lex Nova.

FARALDO CABANA, P. 2010c. De los delitos relativos al mercado y a los consumidores. *Comentarios al Código penal (GÓMEZ TOMILLO, M. (dir.)).* Valladolid: Lex Nova.

FAVA, P. 2009. Giurisprudenza penale, Dogana, Maggioli.

FERNÁNDEZ ALARCÓN, V. 2006. Desarrollo de sistemas de información: una metodología basada en el modelado, Barcelona, Universidad Politécnica de Catalunya.

FERNÁNDEZ MASIÁ, E. y ESPLUGUES MOTA, C. 1996a. La protección de los programas de ordenador en España, Valencia, Tirant lo Blanch.

FERNÁNDEZ MASIÁ, E. y ESPLUGUES MOTA, C. 1996b. La protección internacional de los programas de ordenador, Granada, Comares.

FERNÁNDEZ SÁNCHEZ, M. T. 2000. Protección penal del secreto de empresa, Madrid, COLEX.

FERNÁNDEZ TERUELO, J. G. 2007. Cibercrimen: los delitos cometidos a través de internet -estafas, distribución de pornografía infantil, atentados contra la propiedad intelectual, daños informáticos, delitos contra la intimidad y otros delitos en la Red-, Constitutio Criminalis Carolina.

FERNÁNDEZ TERUELO, J. G. 2011. Derecho penal e internet: Especial consideración de los delitos que afectan a jóvenes y adolescentes, Lex Nova.

FIANDANCA, G. y MUSCO, E. 2013. Diritto penale Parte speciale, Volume II, Tomo Primo, Il delitti contro la persona, Torino, Zanichelli Editore.

FISCHER, T. 2015. § 202a. Strafgesetzbuch mit Nebengesetzen, Beckiche Kurz Kommentare, Band 10, 62. Auflage, München, C.H.BECK.

FLOR, R. 2008. Art. 615 ter CP: natura e funzioni delle misure di sicurezza, consumazione del reato e bene giuridico protetto. *Diritto penale e proceso*.

FLORES PRADA, I. 2012. Criminalidad informática. Aspectos sustantivos y procesales, Valencia, Tirant lo Blanch.

FONDAROLI, D. 1996. La tutela penale dei "beni informatici". *Diritto dell'informazione e dell'informatica*.

FOTI. 2010. Accesso abusivo a sistema informatico o telematico. Un pericoloso "reato di pericolo". *Rivista italiana di diritto e procedura penale*.

FRÍGOLS I BRINES, E. 2010. La protección constitucional de los datos de las comunicaciones: delimitación de los ámbitos de protección del secretos de las comunicaciones y del derecho a la intimidad a la luz del uso de las nuevas tecnologías. *La protección jurídica de la intimidad (BOIX REIG, JAVIER (dir.) y JAREÑO LEAL, ÁNGELES (coord.)*. Madrid: Iustel.

FROSINI, V. 2000. Sull'accesso abusivo a un sistema informatico o telematico. *Cassatione penale,* nº 11.

G-8 MINISTERIAL MEETINGS ON CRIME. 1999. Ministerial Conference of the G-8 Countries on Combating Transnational Organized Crime. Available: http://www.g8.utoronto.ca/adhoc/crime99.htm.

GALÁN MUÑOZ, A. 2009. La internacionalización de la represión y la persecución de la criminalidad informática: un nuevo campo de batalla en la eterna guerra entre prevención y garantías penales. *Revista Penal,* , n.º 24. Julio 2009**,** 90-107.

GALÁN MUÑOZ, A. 2013. ¿Nuevos riesgos, viejas respuestas? Estudio sobre la protección penal de los datos de carácter personal ante las nuevas tecnologías de la información y la comunicación. *Revista General de Derecho Penal,* nº 19.

GALDIERI, P. 1996. La tutela penale del domicilio informatico. Problemi giuridici dell'informatica nel MEC (GALDIERI, PAOLO (dir.)). Milano: Giuffrè.

GALDIERI, P. 1997. Teoria e pratica nell'interpretazione del reato informatico, Milano, Giuffrè.

GALDIERI, P. 2001. L'introduzione contro la volontà del titolare fa scattare la responsabilità dell'hacker. *Guida al diritto,* nº 8.

GARCÍA ALBERO, R. M. 1995. Non bis in idem: material y concurso de leyes penales, Cedecs.

GARCÍA GARCÍA, C. 2003. El derecho a la intimidad y dignidad en la doctrina del Tribunal Constitucional, Murcia, Universidad de Murcia.

GARCÍA GUERRERO, J. L. 2013. *Los derechos fundamentales,* Valencia, Tirant lo Blanch.

GARCÍAS PLANAS, G. 1989. Consecuencias del principio "non bis in idem" en Derecho penal. *Anuario de derecho penal y ciencias penales,* 42**,** 109-124.

GARCÍA VITORIA, A. 1983. El derecho a la intimidad en el Derecho penal y en la Constitución de 1978, Barcelona, Aranzadi.

GAROFOLI, R. 2013. Manuale di Diritto penale. Parte speciale. Tomo II, Roma, Neldiritto editore.

GARRIDO CARRILLO, A. 2006. Fundamentos de programación en C ++, Madrid, Delta Publicaciones.

GARRIGA DOMÍNGUEZ, A. 1999. La protección de los datos personales en el Derecho español, Madrid, Dykinson.

GATTA, G. L. 2011. Capitolo VII Dilitti contro l'inviolabilità del domicilio. *Reati contro la persona e contro il patrimonio* (*Palazzo, Francesco* (Paliero, Carlo Enrico (dir.)). Torino: Giappichelli.

GERCKE, M. y BRUNST, P. 2009. Praxishandbuch Internetstrafrecht, Stuttgart, Kohlhammer.

GEERDS. 1953. Einwilligung und Einverständnis des Verletzten, Kiel: [S.l. : s.n.].

GEERDS. 1954. Einwilligung und Einverständnis des Verletzten, GA.

GEERDS. 1960. Einwilligung und Einverständnis des Verletzten, ZStW, 72.

GIMENO SENDRA, V. 2009. La intervención de las comunicaciones. *Diario La Ley,* nº 7192.

GILI PASCUAL, A. y MONTSERRAT SÁNCHEZ-ESCRIBANO, M. I. 2014. Delitos contra el patrimonio y contra bienes supraindividuales, Palma de Mallorca, Edicions UIB.

GIMBERNAT ORDEIG. 2006 Otra vez: conducta de la víctima e imputación objetiva, Cuadernos de derecho judicial, 93-108, 2006.

GIMBERNAT ORDEIG. 2011. Riesgo permitido y comisión por omisión imprudente: a propósito de la sentencia de 9 de diciembre de 2003, de la Sala III de la Cámara Nacional de Casación Penal argentina, La ley penal: revista de derecho penal, procesal y penitenciario, 4.

GÓMEZ LANZ, J. 2006. La interpretación de la expresión en perjuicio en el código penal, Madrid, Dykinson.

GÓMEZ MARTÍN, V. 2011. Capítulo V. De la usurpación de funciones públicas y del intrusismo. *Comentarios al Código penal (CORCOY BIDASOLO, M. y MIR PUIG, SANTIAGO (dir.))*. Valencia: Tirant lo Blanch.

GÓMEZ NAVAJAS, J. 2005. La protección de los datos personales. Un análisis desde la perspectiva del Derecho penal, Navarra, Thomson Civitas.

GÓMEZ PAVÓN, P. 1989. La intimidad como objeto de protección penal, Madrid, AKAL.

GÓMEZ TOMILLO, M. 2010. Del acoso sexual. Comentarios al Código penal (GÓMEZ TOMILLO, M. (dir.)). Valladolid: Lex Nova.

GÓMEZ RIVERO. 2012. Los delitos contra la propiedad intelectual e inductrial. La tutela penal sobre bienes inmateriales, Valencia: Tirant lo Blanch "Tratados".

GONZÁLEZ CUSSAC, J. L. 2016. Acceso ilícito e intrusismo informático (art. 197 bis), en Derecho penal: Parte Especial (GONZÁLEZ CUSSAC, J.L. (coord.)), Valencia: Tirant lo Blanch.

GONZÁLEZ GUITIÁN, L. 1986. Escuchas clandestinas realizadas por particulares. *Comentarios a la Legislación Penal. Tomo VII.* Madrid: Edersa.

GONZÁLEZ LÓPEZ, J. J. 2007. Los datos de tráfico de las comunicaciones electrónicas en el proceso penal, Madrid, La Ley.

GONZÁLEZ RUS, J. J. 1986a. Aproximación al tratamiento penal de los ilícitos patrimoniales relacionados con medios o procedimientos informáticos. *Revista de la Facultad de Derecho de la Universidad Complutense*, 107-164.

GONZÁLEZ RUS, J. J. 1986b. Tratamiento penal de los ilícitos patrimoniales relacionados con medios o procedimientos informáticos. *Poder Judicial*, 39-52.

GONZÁLEZ RUS, J. J. 1999. Protección penal de sistemas, elementos, datos, documentos y programas informáticos. *Revista electrónica de ciencia penal y criminología* [Online], 1.

GONZÁLEZ RUS, J. J. 2005a. Delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio (II). Allanamiento de morada, domicilio de personas jurídicas y establecimentos abiertos al público. *Derecho penal español : parte especial*.

GONZÁLEZ RUS, J. J. 2005b. Lección 12. Delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio (I). *Derecho penal español: Parte Especial.* Madrid: Dykinson.

GONZÁLEZ RUS, J. J. 2006. Los ilícitos en la red (I): hackers, crackers, cyberpunks, sniffers, denegación de servicio y otros comportamientos semejantes. *El cibercrimen: nuevos retos jurídico-penales, nuevas respuestas político-criminales* Comares.

GONZÁLEZ RUS, J. J. 2007. Precisiones conceptuales y político-criminales sobre la intervención penal en Internet. *Delito e informática: algunos aspectos. Cuadernos penales José María Lidón. Universidad de Deusto*, nº 4.

GONZÁLEZ RUS, J. J. 2011a. Capítulo 14. Delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio (I). *Sistema de Derecho penal Español. Parte Especial (MORILLAS CUEVA, L. (coord.)).* Madrid: Dykinson.

GONZÁLEZ RUS. 2011b Capítulo 15. Delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio (II). Allanamiento de morada, domicilio de personas jurídicas y establecimientos abiertos al público, en Sistema de Derecho penal

Español. Parte Especial (MORILLAS CUEVA, L. (coord.)), Madrid: Dykinson.

GRAF, J.-P. 2012. § 202a. Münchener Kommentar zum Strafgesetzbuch (JOECKS, WOLFGANG y MIEBACH, KLAUS (dir.)), Band 4 §§ 185 bis 262, 2. Auflage. München: Verlag C. H. Beck.

GRIMALT SERVERA, P. 1997. El derecho a controlar los datos personales: algunas consideraciones jurídico-constitucionales (DAVARA RODRÍGUEZ, M. A. (coord.)). *X Años de Encuentros sobre Informática y Derecho 1996-1997, Universidad Pontificia Comillas.* Pamplona: Aranzadi.

GRIMALT SERVERA, P. 2007. La protección civil de los derechos al honor, a la intimidad y a la propia imagen, Madrid, Iustel.

GRÖSELING, N. y HÖFINGER, F. M. 2007. Hacking und Computerspionage - Auswirkungen des 41. StrAndG zur Bekämpfung der Computerkriminalität. *MultiMedia und Recht*.

GUERRERO ZAPLANA, J. 2007. Los delitos contra la propiedad intelectual. Estudios de Derecho Judicial: Propiedad intelectual: aspectos civiles y penales, 129.

GUILLÓ SÁNCHEZ-GALIANO, A. 1996. Intimidad y Familia. Perfiles del Derecho Constitucional a la vida privada y familiar. Madrid: Consejo General del Poder Judicial.

GUTIÉRREZ FRANCÉS, M. L. 1996. El intrusismo informático (hacking): ¿represión penal autónoma? *Informática y derecho: Revista iberoamericana de derecho informático,* Nº 12-15 (Ejemplar dedicado a: II Congreso Internacional de Informática y Derecho. Actas (volumen II)), 1163-1184.

HAFT, F. 1987. Das Zweite Gesetz zur Bekämpfung der Wirtschaftskriminalität. *Neue Zeitschrift für Strafrecht*, nº 2, 6-10.

HEADS OF STATE OF G8 AND THE PRESIDENT OF THE EUROPEAN COMMISSION. 1998. Birmingham Submmit. Available: http://www.g8.utoronto.ca/summit/1998birmingham/finalcom.htm.

HEADS OF STATE OF G8 AND THE PRESIDENT OF THE EUROPEAN COMMISSION. 2000. Okinawa Submmit. Available: http://www.g8.utoronto.ca/summit/2000okinawa/finalcom.htm.

HEFENDEHL, R. 2007. La Teoría del bien jurídico: ¿fundamento de legitimación del Derecho penal o juego de abalorios dogmático?, Marcial Pons, Ediciones Jurídicas y Sociales.

HEGER, M. 2014. § 202a. Strafgesetzbuch Kommentar (LACKNER, KARL y KÜHL, KRISTIAN), 28. Auflage. München: C.H.BECK.

HENKEL 1959. Der Strafschutz des Privatlebens gegen indiskretion. *Verhandlugen des Zweiundvierzigsteb Deutschen Juristentages.* Dusseldorf: Mohr.

HEREDERO HIGUERAS, M. 1996. Ley Orgánica 5/1992, de 29 de octubre, de Regulación del Tratamiento Automatizado de Datos de Carácter Personal. Comentario y textos, Madrid, Tecnos.

HERNÁNDEZ DÍAZ, L. 2010. Aproximación a un concepto de Derecho penal informático. *Derecho penal informático.* Navarra: Thomson Reuters.

HERNÁNDEZ PLASENCIA, J. U. 2004. El delito de allanamiento de morada. Comentarios al Código penal. Parte Especial (DIEZ RIPOLLES, J. L. y ROMEO CASABONA (coord.)). Valencia: Tirant lo Blanch.

HERNÁNDEZ TRASOBARES, A. 2003. Los sistemas de información: evolución y desarrollo. *Proyecto social: Revista de relaciones laborales,* 10-11.

HERRÁN ORTIZ, A. I. 1999. La violación de la intimidad en la protección de datos personales, Madrid, Dykinson.

HERRÁN ORTIZ, A. I. 2003. El derecho a la protección de datos personales en la sociedad de la información, Bilbao, Universidad de Deusto.

HERRERO TEJEDOR, F. 1998. La intimidad como derecho fundamental, Castellón, COLEX.

HERZOG, F. 2009. Straftaten im Internet, Cimputerkriminalität und die Cubercrime Convencion. *Polícita Criminal* [Online], vol. 4 nº 8. Available: http://www.politicacriminal.cl/Vol_04/n_08/Vol4N8D1.pdf.

HILGENDORF, E. 1996. Grundfälle zum Computerstrafrecht. *Juristische Schulung,* nº 2**,** 702-706.

HILGENDORF, F. V. 2005. § 202a. Leipziger Kommentar Grosskommentar §§ 146 bis 222 (JÄHNKE, BURKHARD; LAUFHÜTTE, HEINRICH WILHELM; ODERSKY, WALTER), 12 Auflage. Berlin: Walter de Gruyter.

HIRSCH. 1960. Die lehre von den negativen Tabestansmermalen (Der Irrtum über einen Rechtfertigungsgrund, Bonn.

HOYER, A. 2012. § 202a. Systematischer Kommentar zum Strafgesetzbuch, Band III, §§ 123 - 211, 8. Auflage. Köln: Carl Heymanns Verlag.

HUBMANN, H. 1967 (1ª edición 1953). Das Personlichkeitsrecht, 2, Auflage, Köln/Graz, Böhlau.

HUERTA TOCILDO, S. y ANDRÉS DOMÍNGUEZ, C. 2002. Intimidad e informática. *Revista de Derecho Penal,* nº 6.

IGARTUA ARREGUI, F. 1991. La apropiación comercial de la imagen y el nombre ajeno, Madrid, Tecnos.

JAREÑO LEAL, M. D. L. Á. 1999. Revelación de datos personales, intimidad e informática. *Diario La Ley*.

JAREÑO LEAL, M. D. L. Á. 2008. Intimidad e imagen: los límites de la protección penal, Madrid, Iustel.

JAREÑO LEAL. 2010. Lección XX. Delitos contra la intimidad, el derecho a la propia imagen y a la inviolabilidad del domicilio (2). Allanamiento de morada, en Derecho Penal. Parte Especial. Volumen I. La protección penal de los intereses personales (BOIX REIG, JAVIER (dir.)), Madrid: Iustel, 2010.

JESCHECK y WEIGEND. 2002 Tratado de Derecho Penal. Parte General (Traducción de Miguel Olmedo Cardenete), Granada: Comares.

JESSEN, E. 1994. *Zugangsberechtigung und besondere Sicherung im Sinne von §202a StGB,* Frankfurt/M., Berlin, Bern, New York, Paris, Wien, Peter Lang, Europäische Hochschulschriften: Reihe 2, Rechtswissenschaft. Bd. 1470.

JIMÉNEZ CAMPO, J. 1987. La garantía constitucional del secreto de las comunicaciones. *Revista Española de Derecho Constitucional,* nº 20.

JOECKS, W. 2012. Studien Kommentar zum Strafgesetzbuch, München, C.H.BECK.

JORGE BARREIRO. 1982. La relevancia jurídico-penal del consentimiento del paciente en el tratamiento médico-quirúrgico, Cuadernos de Política Criminal, nº 16.

JORGE BARREIRO, A. 1987. *El Allanamiento de morada*, Tecnos.

JORGE BARREIRO, A. 1997. Delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio. *Comentarios al Código Penal (RODRÍGUEZ MOURULLO, GONZALO (dir.) y JORGE BARREIRO, AGUSTÍN (coord.)).* Madrid: Civitas.

JORGE BARREIRO, A. 1999. Del descubrimiento y revelación de secretos. *Comentarios al Código penal (Cobo del Rosal, M. (dir.))*. Madrid: Edersa.

JORGE BARREIRO, A. 2002. El delito del descubrimiento y la revelación de secretos en el Código Penal de 1995: Un análisis del artículo 197 del CP. *Revista jurídica Universidad Autónoma de Madrid,* nº 6**,** 99-131.

JORGE BARREIRO, A. 2011. Capítulo 27. Delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio. *Memento Penal 2011.* Madrid: Ediciones Francis Lefebvre.

JORGE BARREIRO, A. y RODRÍGUEZ MOURULLO, G. 1997. *Comentarios al Código Penal*, Editorial Aranzadi.

KARAGIANNOPOULOS, V. 2014. From Morris to Nosal: e History of Exceeding Authorization and the Need for a Change, 30 J. Marshall J. Info. Tech. y Privacy L. 465. *The John Marshall Journal of Information Technology y Privacy Law,* 30, 3.

KARGL, W. 2013a. § 202a. Strafgesetzbuch (KINDHÄUSER, URS; NEUMANN, ULFRID; PAEFFGEN, HANS-ULRICH), Band 2, 4 Auflage. Baden Baden: Nomos.

KARGL, W. 2013b. § 202a Strafgesetzbuch (KINDHÄUSER, URS; NEUMANN, ULFRID; PAEFFGEN, HANS-ULRICH), Band 2, 4 Auflage Baden Baden: Nomos.

KASPERSEN, H. 1997. Implementation of Recomendationa (89) 9 on computer-related crime, Strasbourg, Council of Europe.

KERR, O. 2010. Vagueness Challenges to the Computer Fraud and Abuse Act. publicado en 94 Minnesota Law Review 1561, GWU Legal Studies Research Paper No. 482, y GWU Law School Public Law Research Paper No. 482.

KERR, O. 2013. *Computer Crime Law,* St. Paul, Thomson Reuters.

KIENTZY. 1970. Der mangel am Straftatbestand infolge Einwilligung des Rechtsgutstragers, en Auf Grund einer kritischen betrachtung der Differenzierung in Einwilligung ind Enverstandnis, Tübingen: J.C.B. Mohr (Paul Siebeck).

KINDHÄUSER, U. 2013. *Strafgesetzbuch,* Baden-Baden, Nomos.

KLEIN, M. 1997. Klein Einführung in die DIN-Normen, 12. Auflage, Leipzig, Springer Fachmedien Wiesbaden.

KLEINKE, Y. y PURBACH, V. 1993. Information Technology Crime and Criminal Information Law. *Revue Internationale de Droit Penal,* 64.

KRUTISCH, D. 2004. Strafbarkeit des unberechtigten Zugangs zu Computerdaten und -systemen, Schriften zum Strafrecht und Strafprozeßrecht, Frankfurt am Main, Verlag Peter Lang.

KUSNIK, K. 2012. Strafbarkeit der Daten bzw. Informationsspionage in Deutschland und Polen, Baden-Baden, Nomos.

LACKNER, K. y KÜHL, K. 2014. Strafgesetzbuch Kommentar, 28. Auflage, München, C.H.BECK.

LAPIEDRA ALCAMÍ, R., DEVECE CARAÑANA, C. y GUIRAL HERRANDO, J. 2011. *Introducción a la gestión de sistemas de información en la empresa,* Castellón, Publicacions de la Universitat Jaume I, Servei de Comunicació i Publicacions.

LATORRE LATORRE, V. 2014. Protección penal del derecho de autor, Valencia, Tirant lo Blanch.

LATTANZI, G. y LUPO, E. 2010. Codice penale. Rassegna di Giurisprudenza e di Doctrina, Volumen XI, Tomo Secondo, I delitti contro la persona e i delitti contro la libertà individuale, Libro II, Artt. 600-623 bis, Milano, Giuffrè.

LENCKNER, T. y EISELE, J. 2010. § 202a. Strafgesetzbuch (SCHÖNKE, ADOLF y SCHRÖDER, HORST (dir.)), 28. Auflage. München: C.H.BECK.

LEZERTÚA 2002. El proyecto de Convenio sobre el cibercrimen del Consejo de Europa. *Cuadernos de derecho judicial*.

LLORIA GARCÍA, P. 2001. El delito de intrusismo profesional: bien jurídico y configuración del injusto, Valencia: Tirant lo Blanch.

LLORIA GARCÍA, P. 2010. El secreto de las comunicaciones: su interceptación en el ámbito de los delitos cometidos a través de Internet. Algunas consideraciones. *La protección jurídica de la intimidad (BOIX REIG, JAVIER (dir.) y JAREÑO LEAL, ÁNGELES (coord.).* Madrid: Iustel.

LÓPEZ BARJA DE QUIROGA. 1999. El consentimiento en el Derecho penal, Madrid: Dykinson.

LÓPEZ DÍAZ, E. 1996. El derecho al honor y el derecho a la intimidad, Madrid, Dykinson.

LÓPEZ ORTEGA, J. J. 2004. Intimidad informática y derecho penal (la protección penal de la intimidad frente a las nuevas tecnologías de la información y comunicación). *Cuadernos de derecho judicial,* 9 (Ejemplar dedicado a: Derecho a la intimidad y nuevas tecnologías / Carlos Gómez Martínez (dir.)), 107-142.

LÓPEZ YÉPEZ, J. 1991. El desarrollo de los sistemas de información y documentación. *Revista General de Información y Documentación,* 1, 2, 23-34.

LOZANO MIRALLES, J. 1998. Compendio de Derecho penal. Parte Especial II (BAJO FERNÁNDEZ, MIGUEL (dir.)). Madrid: Centro de Estudios Ramón Aceres.

LUBERTO, M. 2008. I reati informatici contro il diritto alla privacy. La tutela fornita dal d. lg. n. 196 del 2003 e dal codice penale. *Giurisprudenza di merito*.

LUSITANO, D. 1998. In tema di accesso abusivo a sistema informatici o telematici. *Giurisprudenza italiana,* nº 3.

LUZÓN PEÑA, D. M. 2013. Consentimiento presunto y autorización oficial: exclusión de la antijuricidad o de la tipicidad y requisitos respectivos. *Revista de Derecho Penal*, 9-33.

MADRID CONESA, F. 1984. Derecho a la intimidad, informática y Estado de derecho, Valencia, Universidad de Valencia.

MAIORANO, N. 2010. Articolo 615 ter Accesso abusivo ad un sistema informatico o telematico. Codice penale. Rassegna di Giurisprudenza e di Doctrina, Volumen XI, Tomo Secondo, I delitti contro la persona e i delitti contro la libertà individuale, Libro II, Artt. 600-623 bis (LATTANZI, GIORGIO y LUPO, ERNESTO (dir.)). Milano: Giuffrè.

MANTOVANI, M. O. 1994. Brevi nota a proposito della nuova legge sulla criminalità informatica. *Critica del Diritto,* 4.

MANTOVANI, F. 1995. Diritto Penale. Parte Speciale I. Delitti contro la persona, Milano, Cedam.

MANTOVANI, F. 2011. Diritto penale. Parte Speciale I. Delitti contro la persona, Padova, CEDAM.

MANZANARES SAMANIEGO, J. L. 1978. El artículo 497 del Código penal. *Anuario de derecho penal y ciencias penales*, XXXI, II.

MARANI, S. 2007. I dellitti contro la persona, Padova, CEDAM.

MARCHENA GÓMEZ, M. 1996. Intimidad e informatica: la proteccion jurisdiccional del "habeas data". *Boletín de Información. Ministerio de Justicia e Interior*.

MARCHENA GÓMEZ, M. 2001. Aspectos penales del tratamiento automatizado de datos. *XIV Encuentros sobre Informática y Derecho : 2000-2001.* Elcano (Navarra) : Aranzadi, 2001.

MARSHALL, J. y BAILI, M. 2011. *Prosecuting Computer Crimes,* United States, Office of Legal Education Executive Office for United States Attorneys.

MARTÍN MORALES, R. 1995. El régimen constitucional del secreto de las comunicaciones, Madrid, Civitas.

MARTÍN-CASALLO LÓPEZ, J. J. 2000. Problemática Jurídica en torno al fenómeno de Internet. *Cuadernos de derecho judicial*.

MARTÍNEZ DE PISÓN CAVERO, J. 1993. El derecho a la intimidad en la jurisprudencia del Tribunal Constitucional, Madrid, Civitas.

MATA Y MARTÍN, R. M. 1997. Bienes jurídicos intermedios y delitos de peligro, Granada, Comares.

MATA Y MARTÍN, R. M. 2001a. Delincuencia informática y Derecho Penal, Madrid, Edisofer.

MATA Y MARTÍN, R. M. 2001b. Delincuencia informática y Derecho Penal, Madrid, Edisofer.

MATA Y MARTÍN, R. M. 2006a. La protección penal de los datos como tutela de la intimidad de las personas. Intimidad y nuevas tecnologías. *Revista Penal,* nº 18.

MATA Y MARTÍN, R. M. 2006b. Perspectivas sobre la protección penal del software. El cibercrimen: nuevos retos jurídico-penales, nuevas respuestas político-criminales. Comares.

MATA Y MARTÍN, R. M. 2007. Protección penal del software. Derecho Penal y Criminología: Revista del Instituto de Ciencias Penales y Criminológicas, 28**,** 81-106.

MATA Y MARTÍN, R. M. 2014. Capítulo II. De los Robos. Comentarios al Código penal (GÓMEZ TOMILLO, M. (dir.)). Valladolid: Lex Nova.

MATELLANES RODRÍGUEZ, N. 2000. Algunas notas sobre las formas de delincuencia informática en el Código Penal. *Hacia un derecho penal sin fronteras.* Madrid: Colex, 2000.

MATELLANES RODRÍGUEZ, N. 2004. El intrusismo informático como delito autónomo. *Revista General de Derecho Penal,* nº 2.

MATELLANES RODRÍGUEZ, N. 2008. Vías para la tipificación del acceso ilegal a los sistemas informáticos. *Revista Penal,* nº 22.

MAYO CALDERÓN, B. 2005. La tutela de un bien jurídico colectivo por el delito societario de administración fraudulenta. Estudio del artículo 195 del Código penal español y propuesta de lege ferenda, Granada, Comares.

MELONI, M. 2012. 615 ter Accesso abusivo ad un sistema informatico o telematico. *Codice Penale Commentato (RONCO, MAURO y ROMANO; BARTOLOMEO (dir.)).* Torino: UTET.

MENDEZ REBOLLAL, A. 2007. Delitos contra la propiedad intelectual relativos a programas de ordenador. Aspectos prácticos. *La Ley Penal,* 34.

MENDOZA BUERGO, B. 2001. Límites dogmáticos y político-criminales de los delitos de peligro abstracto, Granada, Comares.

MENÉNDEZ, V. 1994. Protección de datos personales, derecho a ser informado y autodeterminación informativa. A propósito de la STC 254/1993, de 20 de julio. *Revista española de Derecho constitucional,* nº 41.

MERLI, A. 1993. Il diritto penale dell'informatica: legislatione vigente e prospettive di riforma. *Giurisprudenza penale,* II.

MEURER, D. 1992. Die Bekämpfung der Computerkriminalität in der Bundesrepublik Deutschland. *Wege zum japanischen Recht: Festschrift für Zentaro Kitagawa*, 971-986.

MIERES MIERES, L. J. 2002. Intimidad personal y familiar. Prontuario de Jurisprudencia Constitucional, Navarra, Aranzadi.

MIR PUIG, C. 2002. Sobre algunas cuestiones relevantes del derecho penal en internet. *Cuadernos de derecho judicial,* X.

MIR PUIG, S. 2005. Derecho penal. Parte General. 7ª Edición, Barcelona, Reppertor.

MIRÓ LLINARES, F. 2004. La protección penal de los derechos de explotación exclusiva sobre el software. *Revista Penal,* 3**,** 85 - 104.

MIRÓ LLINARES, F. 2005. Internet y delitos contra la propiedad intelectual, Madrid, Fundación Autor.

MIRÓ LLINARES, F. 2007. Sobre la posible concurrencia y compatibilidad de tutelas penales de propiedad industrial e intelectual sobre un mismo objeto. *Eguzkilore: Cuaderno del Instituto Vasco de Criminología,* 21**,** 95-115.

MIRÓ LLINARES, F. 2010. Capítulo 6. Delitos informáticos: Hacking. Daños. *Memento Experto. Reforma penal 2010.* Madrid: Ediciones Francis Lefebvre.

MIRÓ LLINARES, F. 2016. Capítulo 6. Delitos informáticos: Hacking. Daños. *Memento penal.* Madrid: Ediciones Francis Lefebvre.

MOLINA JIMENO, F. J. 2009. El hacking ¿una conducta punible? *Diario La Ley,* nº 7131.

MONACO, L. 2011. Articulo 615 ter. Comentario breve al Codice Penale (CRESPI, ALBERTO; FORTI, GABRIO; y ZUCCALÀ, GIUSEPPE). Padova: CEDAM.

MONTERO CARRIÓN, J. J. 2008. Distinguir entre Sistemas de Información y Sistemas Informáticos. *Partida Doble,* 195**,** 76-81.

MONTSERRAT SÁNCHEZ-ESCRIBANO, M. I. 2014. Panorama normativo supranacional del delito de acceso ilícito a un sistema informático, en Investigaciones en ciencias jurídicas: desafíos actuales del derecho (VALENCIA SÁIZ, ÁNGEL (coord.)), Málaga: eumed.net.

MONTSERRAT SÁNCHEZ-ESCRIBANO, M. I. 2014. El objeto material en el artículo 197.3 del código penal: un condicionante de la

tutela de la seguridad en España, en Moderno discurso penal y nuevas tecnologías: memorias [del] III Congreso Internacional de Jóvenes Investigadores en Ciencias Penales, 17, 18 y 19 de junio de 2013 (DIAZ CORTES, LINA MARIOLA y PÉREZ ÁLVAREZ, FERNANDO (coords.), 233-254, Salamanca: Ediciones Universidad de Salamanca.

MONTSERRAT SÁNCHEZ-ESCRIBANO, M. I. 2015. Libertad informática y protección de datos: desarrollo en la jurisprudencia del Tribunal Constitucional y tutela penal en el delito de descubrimiento y revelación de secretos. *Anuario de Derecho y Justicia constitucional*, 19.

MONTSERRAT SÁNCHEZ-ESCRIBANO, M. I. 2015. El nuevo apartado 3 del artículo 197 del Código penal: análisis e la transposición en el ámbito español del delito de acceso ilícito a un sistema informático, *Revista Peruana de Ciencias Penales*, 295-322.

MORALES GARCÍA, Ó. 2002. Apuntes de política criminal en el contexto tecnológico. Una aproximación a la Convención del Consejo de Europa sobre Cyber-crime. *Cuadernos de derecho judicial,* IX.

MORALES GARCÍA, Ó. 2003. Política criminal en el contexto tecnológico. Una aproximación a la Convención del Consejo de Europa sobre delincuencia informática. Available: http://www.uoc.edu/in3/dt/20285/20285.pdf.

MORALES GARCÍA, Ó. 2010. Delincuencia informática: intrusismo, sabotaje informático y uso ilícito de tarjetas (arts. 197.3 y 8, 264 y 248). *La reforma penal de 2010: análisis y comentarios (QUINTERO OLIVARES (dir.))*. Navarra: Aranzadi.

MORALES GARCÍA, Ó. 2012. Comentario a los delitos informáticos de los artículos 197, 248 y 264 del Código penal. *Delincuencia informática. Tiempos de cautela y amparo*. Navarra: Thomsons Reuters Aranzadi.

MORALES LÓPEZ, V. 2010. La perspectiva organizacional de los sistemas de información. *Documentación de las Ciencias de la Información,* 33**,** 142-169.

MORALES PRATS, F. 1984. La tutela penal de la intimidad: privacy e informática, Destino.

MORALES PRATS, F. 1996. Los delitos contra la intimidad en el código penal de 1995: reflexiones político-criminales *Estudios de derecho judicial,* Nº. 2 (Ejemplar dedicado a: Estudios sobre el Código Penal de 1995 (parte especial) / José Luis Manzanares Samaniego (dir.), Tomás Salvador Vives Antón (dir.))**,** 239-282.

MORALES PRATS, F. 2010. Del allanamiento de morada, domicilio de personas jurídicas y establecimientos abiertos al público. *Comentarios a la Parte Especial del Derecho penal (QUINTERO OLIVARES (dir.) y MORALES PRATS (coord.)).* Navarra: Thomson Reuters.

MORALES PRATS, F. 2011a. Delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio. *Comentarios a la Parte Especial del Derecho penal (QUINTERO OLIVARES (dir.) y MORALES PRATS (coord.)).* Navarra: Thomson Reuters.

MORALES PRATS, F. 2011b. El delito de acceso ilícito a los sistemas informáticos (art. 197.3) y la proyección de la responsabilidad de las persona jurídicas a los delitos contra la intimidad: una primera acotación a la Reforma penal de 2010. *Un Derecho penal comprometido. Libro homnaje al profesor Dr. Gerardo Landrove Díaz.* Tirant lo Blanch.

MORALES PRATS, F. y GARCÍA SOLÉ, M. 2010. Título XVII De los delitos contra la seguridad colectiva. Capítulo I. De los delitos de riesgo catastrófico. Sección 1ª. De los delitos relativos a la energía nuclear y a las radiaciones ionizantes., Navarra, Thomson-Reuters.

MORALES PRATS, F. 2015. La reforma de los delitos contra la intimidad artículo 197 CP, en Comentario a la reforma penal de 2015

(QUINTERO OLIVARES, GONZALO (dir.)), 459-467, Navarra: Aranzadi.

MORALES PRATS, F. y MORÓN LERMA, E. 2011. Artículo 278. Comentarios a la Parte Especial del Derecho penal (QUINTERO OLIVARES (dir.) y MORALES PRATS (coord.)). Navarra: Thomson Reuters.

MORANT VIDAL, J. 2003. Protección penal de la intimidad frente a las nuevas tecnologías: estudio de los artículos 197 a 201 del Código penal, Valencia, Práctica de Derecho.

MORETÓN TOQUERO, M. A. 2002. Delitos contra la propiedad intelectual, Madrid, Bosch.

MORÓN LERMA, E. 2001. Intención del agresor y ataque a la intimidad. El nuevo Derecho penal español: Estudios penales en memoria del Profesor José Manuel Valle Muñiz (QUINTERO OLIVARES, GONZALO (dir.) y MORALES PRATS (coord.)). Navarra: Aranzadi.

MORÓN LERMA, E. 2002a. Internet y derecho penal: hacking; y otras conductas ilícitas en la red, Navarra: Aranzadi.

MORÓN LERMA, E. 2002b. La tutela penal del secreto de empresa, desde una teoría general del bien jurídico. Tesis doctoral: Universidad de Barcelona.

MORÓN LERMA, E. 2002 y 1999. Internet y derecho penal: hacking; y otras conductas ilícitas en la red, Navarra: Aranzadi.

MOYA FUENTES, M. D. M. 2010. El nuevo delito de acceso ilícito a sistemas informáticos: art. 197.3 CP. *Revista General de Derecho Penal*.

MUCCIARELLI, F. 1996. Commento all'art. 4 della lege n. 547 del 1993. *Legislazione penale*.

MUÑOZ CONDE, F. J. 1971. El delito de alzamiento de bienes, Barcelona, Bosch.

MUÑOZ CONDE, F. J. 2010. Derecho penal. Parte Especial, Valencia, Tirant lo Blanch.

MUÑOZ CONDE, F. J. 2015. Derecho penal. Parte Especial, Valencia, Tirant lo Blanch.

MURILLO DE LA CUEVA, P. L. 1991. El derecho a la autodeterminación informativa: la protección de los datos personales frente al uso de la informática, Tecnos.

MURILLO DE LA CUEVA, P. L. 1993. Informática y protección de datos personales: (estudio sobre la Ley Orgánica 5/1992, de regulación del tratamiento automatizado de los datos de carácter personal), Centro de Estudios Constitucionales.

MURILLO DE LA CUEVA, P. L. 2009. La protección de los datos de carácter personal en el horizonte de 2010. *Anuario de la Facultad de Derecho*, 131-142.

NILSON, H. 1993. Computer Crimes and Other Crimes against Information Technology within the Wirking Programme of the Council of Europe. *Revue Internationale de Droit Penal,* 64.

NULL, L. y LOBUR, J. 2015. The Essentials of Computer Organization and Architecture, Fourth Edition, USA, Jones y Barlett.

NUNZIATA, M. 1996. Il delito di acceso abusivo ad un sistema informatico o telematico.

NUNZIATA, M. 1998. La prima applicazione giurisprudenziali del delito di accesso abusivo ad un sistema informatico ex art. 615 ter. *Giurisprudenza di merito*.

NÚÑEZ CASTAÑO. 2010. Lección XII Delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio, en Nociones Fundamentales de Derecho Penal. Parte Especial, Madrid: Tecnos.

O'CALLAGHAN MUÑOZ, X. 1991. Libertad de expresión y sus límites: honor, intimidad e imagen, Madrid, Edersa.

OCDE 1986. Computer-related crime: analysis of legal policy, OECD.

OLIVER LALANA, Á. D. 2002. El derecho fundamental "virtual" a la protección de datos. Tecnología transparente y normas privadas. *La Ley*.

OLIVEROS LAPUERTA, M. V. 1980. Estudio sobre la Ley de Protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen, Madrid, Presidencia del Gobierno, Secretaría General Técnica, Subdirección de Documentación.

OLMO FERNÁNDEZ-DELGADO, L. 2009. El descubrimiento y revelación de secretos documentales y de las telecomunicaciones. Estudio del artículo 197.1 del Código penal, Madrid, Dykinson.

ORGANIZACIÓN MUNDIAL DE LA PROPIEDAD INTELECTUAL. 1978. Dispositions Types sur le protection du logiciel. Available: ftp://ftp.wipo.int/pub/library/ebooks/ModelLaws/loi-type-protection-logiciel-wipopub814f.pdf.

ORTÍ VALLEJO, A. D. P. 1994. Derecho a la intimidad e informática. Tutela de la persona por el uso de ficheros y tratamientos informáticos de datos personales. Particular atención a los ficheros de titularidad privada, Granada, Comares.

ORTIZ DE URBINA GIMENO. 2008. De moscas y agresores muertos: Argumentos a favor de una teoría jurídica del delito bipartita más allá (y a pesar de) la teoría de los elementos negativos del tipo, Indret: Revista para el Análisis del Derecho.

ORTIZ PRADILLO, J. C. 2011. "Hacking" legal al servicio de la investigación criminal: nuevos instrumentos para la investigación y prueba de la delincuencia informática. *Revista de derecho y proceso penal*, 67-92.

ORTIZ PRADILLO, J. C. 2012. "Hacking" legal al servicio de la investigación criminal: nuevos instrumentos para la investigación y prueba de la delincuencia informática. *Delincuencia informática: tiempos de cautela y amparo.* Navarra: Cizur Menor: Thomson Reuters-Aranzadi.

ORTS BERENGUER, E. y ROIG TORRES, M. 2001. Delitos informáticos y delitos comunes cometidos a través de la informática, Valencia, Tirant lo Blanch "Colección los delitos".

ORTS BERENGUER, E. y ROIG TORRES, M. 2005. Delitos contra la intimidad, utilización fraudulenta de tarjetas de crédito y falsedad en documento electrónico: Análisis de casos. *Estudios de derecho judicial,* 71.

PALAZZO, F. y PALIERO, C. E. 2011. Reati contro la persona e contro il patrimonio, Torino, Giappichelli.

PARDO FALCÓN, J. 1992. Los derechos del artículo 18 de la Constitución española en la jurisprudencia del Tribunal Constitucional. *Revista Española de Derecho Constitucional,* nº 34.

PAREJO ALFONSO, L. 1997. El derecho fundamental a la intimidad y sus restricciones. *Cuadernos de Derecho Judicial,* XXII.

PARODI, C. 1998. Accesso abusivo, frode informatica, rivelazione di documenti informatici segreti: rapporti da interpretare. *Diritto penale e proceso,* nº 4**,** 1038-1041.

PARODI, C. 2000. Profili penali dei virus informatici. *Diritto penale e proceso*.

PARODI, C. y CALICE, A. 2001. Responsabilità penali e Internet. Le ipotesi di responsabilità penale nell'uso dell'informatica e della telematica, Milano, Il Sole 24 ORE.

PASCUAL MEDRANO, A. 2003. El derecho fundamental a la propia imagen, Navarra, Thomson Aranzadi.

PATTERSON, D. y HENNSSY, J. 2014. Computer Organization and Design: The hardware/Software Interface, USA, Morgan Kaufmann.

PAZIENZA, F. 1995. In tema di criminalità informatica: l'art. 4 della legge 23 dicembre 1993, n. 547. *Rivista italiana di diritto e procedura penale*.

PECORELLA, C. 2006. Il diritto penale dell'informatica, Padova, CEDAM.

PECORELLA, C. 2011. Codice penale commentato (DOLCINI, EMILIO y MARINUCCI, GIORGIO (dir.)). Milano: IPSOA.

PÉREZ LUÑO, A. E. Intimidad y protección de datos personales: del habeas corpus al habeas data. *Estudios sobre el derecho a la intimidad.*

PÉREZ LUÑO, A. E. 1984. Derechos humanos, Estado de Derecho y Constitución, Madrid, Tecnos.

PETRINI, D. 2004. La responsabilità penale per i reati via Internet, Torino, Jovene.

PICA, G. 1999. Diritto penale delle tecnologie informatiche. Computer's crimes e reati telematici, Internet, banche-date e privacy, Torino, UTET.

PICOTTI, L. 2000. voz Reati informatici. *Enciclopedia giuridica.* Roma: Treccani.

PICOTTI, L. 2004a. Il Diritto penale dell'informatica nell'epoca di Internet, Padova, CEDAM.

PICOTTI, L. 2004b. Sistematica dei rati informatici, rechniche di formulazione legislativa e beni giuridici tutelati. *Il diritto penale dell'informatica nell'epoca di Internet (PICOTTI, LORENZO (dir.)).* Padova: CEDAM.

PICOTTI, L. 2006. Internet y Derecho Penal: ¿un empujón únicamente tecnológico a la armonización internacional? *El*

cibercrimen: nuevos retos jurídico-penales, nuevas respuestas político-criminales Granada: Comares.

PICOTTI, L. y SALVADORI, I. 2008. National legislation implementing the Convention on Cybercrime - Comparative analysys and good practices, Strasbourg, Economic Crime Division. Directorate General of Human Rights and Legal Affairs.

PIÑAR MAÑAS, J. L. 2010. Concepto de dato de carácter personal. Comentarios a la Ley Orgánica de protección de datos de carácter personal (TRONCOSO REIGADA, ANTONIO (dir.)). Navarra: Thomson Reuters.

PLANTAMURA, V. 2006a. La tutela penale delle comunicazioni informatiche e telematiche. *Diritto dell'informazione e dell'informatica*.

PLANTAMURA, V. 2006b. Moderne tecnologie, riservatezza e sistema penale: quali equilibri? *Diritto dell'informazione e dell'informatica*.

PLANTAMURA, V. y MANNA, A. 2007. *Diritto penalle e informatica,* Bari, Cacucci Editore.

POLAINO NAVARRETE. 1974. El bien jurídico en el Derecho penal, Anales de la Universidad Hispalense, Serie Derecho, nº 19.

POLAINO NAVARRETE, M. 1997. Delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio (I). Descubrimiento y revelación de secretos. *Derecho penal español. Parte Especial I (COBO DEL ROSAL (dir.)).* Madrid: Marcial Pons.

PORTILLA CONTRERAS, G. 1989. Principio de intervención mínima y bienes jurídicos colectivos. *Cuadernos de política criminal*, 723-748.

PUENTE ABA, L. M. 2004. Propuestas internacionales de criminalizar el acceso ilegal a sistemas informáticos: ¿debe protegerse de forma autónoma la eguridad informática? *Nuevos retos del derehco*

penal en la era de la globalización (FARALDO CABANA, P. dir.). Tirant lo Blanch.

PUENTE ABA, L. M. 2007. Delitos contra la intimidad y nuevas tecnologías. *Eguzkilore: Cuaderno del Instituto Vasco de Criminología,* 21**,** 163-183.

QUERALT JIMÉNEZ, J. J. 2010. Derecho penal. Parte Especial, Barcelona, Atelier.

QUINTANO RIPOLLÉS. 1972. Tratado de la Parte Especial del Derecho penal, Madrid: Edersa.

QUINTERO OLIVARES, G. 1973. *El alzamiento de bienes,* Barcelona, Praxis.

QUINTERO OLIVARES, G. 2001. Internet y propiedad intelectual. *Cuadernos de derecho judicial,* nº 10 (Ejemplar dedicado a Internet y Derecho penal (LÓPEZ ORTEGA, JUAN JOSÉ (dir.)), 367-398.

QUINTERO OLIVARES. 2008. Título XIII. Delitos contra el patrimonio y contra el orden socio-económico, en Comentarios a la Parte Especial del Derecho penal (QUINTERO OLIVARES, GONZALO (dir.)), Valencia: Tirant lo Blanch.

RAGUÉS I VALLÈS, R., ROBLES PLANAS, R. y SILVA SÁNCHEZ, J. M. 2012. Capítulo 13. La reforma de los delitos informáticos: Incriminación de los ataques a sistemas de información. *El nuevo Código Penal: comentarios a la reforma.* Madrid : La Ley, 2012.

REBOLLO DELGADO, L. 2000. El derecho fundamental a la intimidad, Madrid, Dykinson.

REBOLLO VARGAS, R. 2004. Título X. Delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio. *Comentarios al Código penal. Parte Especial. Tomo I (CÓRDOBA RODA, JUAN y GARCÍA ARÁN, MERCEDES (dir.)).* Madrid y Barcelona: Marcial Pons y Ediciones Jurídicas y Sociales.

RELLA, M. 2007. La violazione del domicilio informatico. Diritto penalle e informatica (PLANTAMURA, VITO y MANNA, ADELMO (dir.)). Bari: Cacucci Editore.

ROBLES PLANAS, R. 2012. Los dos niveles del sistema de intervención en el delito: (El ejemplo de la intervención por omisión). *Indret: Revista para el Análisis del Derecho*.

ROBLES PLANAS, R. y PASTOR MUÑOZ, N. 2012. Tema 12. Delitos contra el patrimonio (III). *Lecciones de Derecho penal. Parte Especial (SILVA SÁNCHEZ, JESÚS MARÍA (dir.)).* Barcelona: Atelier.

RODRÍGUEZ GÓMEZ, C. 2003. Criminalidad y sistemas informáticos. *El sistema penal frente a los retos de la nueva sociedad.*

RODRÍGUEZ LAINZ, J. L. 2011. Estudio sobre el secreto de las comunicaciones. Perspectiva doctrinal y jurisprudencial, Madrid, La Ley.

RODRÍGUEZ MONTAÑÉS, T. 1994. *Delitos de peligro, dolo e imprudencia,* Madrid, Centro de Estudios Judiciales Ministerio de Justicia y Servicio de Publicaciones Universidad Complutense Madrid.

RODRÍGUEZ MORO, L. 2011. Delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio. *Lecciones y materiales para el estudio del derecho penal.* Madrid: Iustel.

RODRÍGUEZ MOURULLO. 1982 Consideraciones generales sobre la exclusión de la antijuridicidad, en Libro homenaje al Profesor Antón Oneca, Salamanca: Universidad de Salamanca.

RODRÍGUEZ PADRÓN, C. 1998. La protección del domicilio. Consejo General del Poder Judicial. Ejemplar dedicado a Derecho al honor, a la intimida y a la propia imagen II**,** 85-130.

RODRÍGUEZ RUIZ, B. 1998. El secreto de las comunicaciones: tecnología e intimidad, Sevilla, McGraw-Hill.

ROMEO CASABONA, C. M. 1988a. La protección penal del software. *Actualidad penal*, nº 35.

ROMEO CASABONA, C. M. 1988b. Poder informático y seguridad jurídica. La función tutelar del derecho penal ante las Nuevas Tecnologías de la Información, FUNDESCO.

ROMEO CASABONA, C. M. 1993. Tendencias actuales sobre las formas de protección jurídica ante las nuevas tecnologías. *Poder Judicial*, nº 31.

ROMEO CASABONA, C. M. 2003a. La intimidad y los datos de carácter personal como derechos fundamentales y como bienes jurídicos penalmente protegidos. *Estudios Jurídicos en Memoria de José María Lidón.* Bilbao: Universidad de Deusto.

ROMEO CASABONA, C. M. 2003b. La intimidad y los datos de carácter personal como derechos fundamentales y como bienes jurídicos penalmente protegidos. *Datospersonales.org: La revista de la Agencia de Protección de Datos de la Comunidad de Madrid*.

ROMEO CASABONA, C. M. 2004a. El delito de descubrimiento y revelación de secretos. Comentarios al Código Penal. Parte Especial II (DIEZ RIPOLLÉS, J. L. y ROMEO CASABONA, C. M. (coord.)). Valencia: Tirant lo Blanch.

ROMEO CASABONA, C. M. 2004b. Los delitos de descubrimiento y revelación de secretos, Valencia, Tirant lo Blanch "Colección los Delitos".

ROMEO CASABONA, C. M. 2006. Los datos de carácter personal como bienes jurídicos penalmente protegidos. *El cibercrimen: nuevos retos jurídico-penales, nuevas respuestas político-criminales* Comares.

ROS GARCÍA, J. 1996. Análisis y planificación de Sistemas de Información: tipología y aplicación a la gestión de la información. *Scire: Representación y organización del conocimiento*, 2, 2**,** 35-52.

ROVIRA DEL CANTO, E. 2002. Delincuencia informática y fraudes informáticos, Comares.

ROVIRA SUEIRO, M. E. 1999. El derecho a la propia imagen. Especialidades de la responsabilidad civil en este ámbito, Madrid, Comares.

ROVIRA VIÑAS, A. 1992. Reflexiones sobre el derecho a la intimidad en relación a la informática, la medicina y los medios de comunicación. *Revista de estudios políticos*, 259-266.

ROXIN. 1997. Derecho Penal. Parte General. Tomo I. Fundamentos. La Estructura de la Teoría del Delito (Traducción de Diego-Manuel Luzón Peña, Miguel Díaz y García Conlledo y Javier de Vicente Remesal), Navarra: Thomson Civitas.

RUDOLPHI, H. J., HORN, GÜNTHER y SAMSON *STGB*, Luchterhand.

RUEDA MARTÍN, M. A. 2004a. Protección penal de la intimidad informática: Los delitos de descubrimiento y revelación de secretos de los artículos 197 y 198 del Código penal, Atelier.

RUEDA MARTÍN, M. D. L. Á. 2004b. Protección penal de la intimidad personal e informática (Los delitos de descubrimiento y revelación de secretos de los artículo 197 y 198 del Código penal), Alicante, Atelier.

RUEDA MARTÍN, M. Á. 2010. Los ataques contra los sistemas informáticos: Conductas de hacking. Cuestiones político-criminales. *La adaptación del Derecho penal al desarrollo social y tecnológico.* Comares.

RUIZ MARCO, F. 1999. Artículo 197. Comentarios al Código penal (Cobo del Rosal, M. (dir.)). Madrid: Edersa.

RUIZ MARCO, F. 2001. Los delitos contra la intimidad: especial referencia a los ataques cometidos a través de la informática, COLEX.

RUIZ MIGUEL, C. 1995. La configuración constitucional del derecho a la intimidad, Tecnos.

RUIZ VADILLO, E. 1989. Tratamiento de la delincuencia informática como una de las expresiones de la criminalidad económica. *Poder Judicial*, 53-84.

SALVADORI, I. 2012. Los nuevos delitos informáticos introducidos en el Código Penal Español con la Ley Orgánica n. 5/2010 (PÉREZ ÁLVAREZ, FERNANDO (dir.)). Delito, pena, política criminal y tecnologías de la información y la comunicación en las modernas ciencias penales: memorias II Congreso Internacional de Jóvenes investigadores en Ciencias Penales 27, 28 y 29 de junio de 2011 (PÉREZ ÁLVAREZ, FERNANDO (dir.)). Salamanca: Ediciones Universidad de Salamanca.

SÁNCHEZ BRAVO, A. A. 1998. *La protección del derecho a la libertad informática en la Unión Europea*, Sevilla : Universidad de Sevilla, Secretariado de Publicaciones, 1998.

SÁNCHEZ DE DIEGO FERNÁNDEZ DE LA RIVA, M. 1996. Criterios delimitadores de lo público y lo privado. *Sobre la intimidad (VALLÉS COPEIRO DEL VILLAR, ANTONIO y AZNAR GÓMEZ, HUGO (coord.)).* Valencia: Fundación Universitaria CEU San Pablo.

SÁNCHEZ DOMINGO, M. B. 2012. 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. *Revista General de Derecho Penal*.

SÁNCHEZ-CALERO ARRIBAS, B. 2011. Honor, intimidad e imagen en el deporte, Madrid, Reus.

SANZ MORÁN, Á. J. 1986. El concurso de delitos. Aspectos de política legislativa., Valladolid, Universidad de Valladolid.

SANZ MORÁN, Á. J. 2006. El allanamiento de morada, domicilio de personas jurídicas y establecimientos abiertos al público, Valencia, Tirant lo Blanch "Colección los delitos".

SCHJOLBERG, S. 2008. The history of global harmonization on cybercrime legislation - The road to Geneva. Available: www.cybercrimelaw.net/documents/cybercrime_history.pdf.

SCHMID, P. 2001. Computerhacken und materielles Strafrecht: unter besonderer Berücksichtigung von § 202a StGB, Dissertation.

SCHMITZ, R. 1995. Ausspähen von daten. *Juristische Arbeitsblätter*.

SCHÖNKE, A. y SCHRÖDER, H. 2010. *Strafgesetzbuch,* München, C.H.BECK.

SCHREIBAUER, M. y HESSEL, T. J. 2007. Das 41. Strafrechtsänderungsgesetz zur Bekämpfung der Computerkriminalität. *Kommunikation y Recht*, 616 - 619.

SCHUHR, J. 2010. Anmerkung zum Beschluss des BGH vom 06.07.2010, Az.: 4 StR 555/09 (Ausspähen von Daten - Herstellen von Kartendubletten). *Neue Zeitschrift für Strafrecht,* nº 3, 155-156.

SCHULTZ, A., SCHRÖNKE y SCHRÖDER § 202 a).

SCHULZE-HEIMING, I. 1995. Der strafrechtliche Schutz der Computerdaten gegen die Angriffsformen der Spionage, Sabotage und des Zeitdiebstahls, Münster/New York, Waxmann.

SCHUMANN, K. H. 2007. Das 41. StrÄndG zur Bekämpfung der Computerkriminalität. *Neue zeitschrift für strafrecht,* 27, 12, 675-680.

SCHÜNEMANN, B. 2000a. § 202a. Leipziger Kommentar Grosskommentar §§ 146 bis 222 (JÄHNKE, BURKHARD; LAUFHÜTTE, HEINRICH WILHELM; ODERSKY, WALTER), 11 Auflage. Berlin: Walter de Gruyter.

SCHÜNEMANN, B. 2000b. § 202a. Leipziger Kommentar Grosskommentar, Jähnke, Laufhütte, Odersky. Walter de Gruyter.

SCHÜNEMANN, B. 2002. ¿Ofrece la reforma del Derecho penal económico alemán un modelo o un escarmiento? *Temas actuales y permanentes del Derecho penal después del Milenio.* Madrid: Tecnos.

SECRETARIAT UNITED NATIONS 1990a. Report to 8th Congress on the Prevention of Crime and the treatment of Offenders, New York, United Nations.

SECRETARIAT UNITED NATIONS 1990b. Report to 9th Congress on the Prevention of Crime and the treatment of Offenders, New York, United Nations.

SECRETARIAT UNITED NATIONS 1990c. Report to 10th Congress on the Prevention of Crime and the treatment of Offenders: Crimes related computer networks, New York, United Nations.

SECRETARIAT UNITED NATIONS 1994. United Nations Manual on the prevention and control of computer-related crime. *International Review of Criminal Policy,* 43 - 44.

SEGRELLES DE ARENAZA, Í. 1996. Derecho penal español. Parte Especial I (COBO DEL ROSAL (dir.)). Madrid: Marcial Pons.

SEGRELLES DE ARENAZA, Í. 2000. Compendio de Derecho penal Español, Madrid, Marcial Pons.

SEGURA GARCÍA. 1999. El consentimiento del titular del bien jurídico en derecho penal: naturaleza y eficacia, Tirant lo Blanch.

SENIOR EXPERTS GROUP ONTRANSNATIONAL ORGANIZED CRIME G7 + RUSSIA. 1996. Senior Experts Group Recommendations to Combat Transnational Organized Crime efficiently. Available: http://www.g8.utoronto.ca/crime/40pts.htm.

SERRANO GONZÁLEZ DE MURILLO, J. L. 1999. Los delitos de incendio. Técnicas de tipificación del peligro en el nuevo Código penal, Barcelona, Marcial Pons.

SERRANO GÓMEZ y SERRANO MAÍLLO. 2011 Derecho Penal. Parte Especial, Madrid: Dykinson.

SIEBER, U. 1977. Computerkriminalität und Strafrecht, Heymann.

SIEBER, U. 1992. Documentación para una aproximación al delito informático. *Delincuencia informática.* PPU.

SIEBER, U. 2012. Straftaten und Strafverfolgung im Internet, München, Verlag C. H. Beck.

SILVA SÁNCHEZ, J. M. 2001. La expansión del derecho penal, Madrid: Civitas.

SOLA RECHE, E. 1991. La protección penal de la intimidad informática. *Anales de la Facultad de Derecho*, 179-198.

SOTO NAVARRO, S. 2003. La protección penal de los bienes colectivos en la sociedad moderna, Granada, Comares.

SOTO NIETO, F. 2001. Delito informático. Acceso y obtención de datos personales. *Diario La Ley*.

SOTO NIETO, F. 2004. Revelación de secretos. Entidad del dato revelado. *Diario La Ley nº 6132*.

STALLINGS, W. 2013. Computer Organization and Architecture Designing for Performance, New Yersey, Prentice Hall. Pearson Education.

STEINMÜLLER, W., LUTTERBECK, B., MALLMANN, C., HARBORT, U., KOLB, G. y SCHNEIDER JOCHEN 1971 y 1972. Grundfragen des Datenschutzes, Bundestagsdrucksache VI/3826 Bonn: Heger.

STERNBERG-LIEBEN, D. 2007. Bien jurídico, proporcionalidad y libertad del legislador penal. La Teoría del bien jurídico: ¿fundamento de legitimación del Derecho penal o juego de abalorios dogmático? : Madrid : Marcial Pons, 2007.

SUÁREZ MONTES 1968. El delito de allanamiento de morada. *Revista General de Legislación y Jurisprudencia*.

SUÁREZ-MIRA RODRÍGUEZ, C. y PIÑOL RODRÍGUEZ, J. R. 2012. *Descubrimiento y revelación de secretos,* Navarra, Aranzadi.

SUBGROUP ON HICH-TECH CRIME G7 + RUSSIA. 1997. Principles and Action Plan to combat High-Tech Crime. *Meeting of the Justice and Interior Ministers of The Eight* [Online]. Available: http://www.g8.utoronto.ca/justice/index.html y http://cryptome.org/jya/g8crime-doj.htm.

TAG, B. 2013. § 202a. Gesamtes Strafrecht, Handkommentar (DÖLLING, DIETER; DUTTGE, GUNNAR y RÖSSNER, DIETER), 3. Auflage. Baden-Baden: Nomos.

TÉLLEZ AGUILERA, A. 2001. Nuevas tecnologías, intimidad y protección de datos, Madrid, Edisofer.

TERRADILLOS BASOCO, J. M. 2001. Peligro abstracto y garantías penales. El nuevo Derecho penal español. Estudios penales en memoria del Profesor José Manuel Valle Muñiz. Navarra: Aranzadi.

TEWARI, D. R., SASTRY, P. K. y RAVIKUMAR, K. V. 2002. *Computer crime and computer forensics,* New Delhi, Select Publishers.

TOMÁS - VALIENTE LANUZA, C. 2010. Del descubrimiento y revelación de secretos. *Comentarios al Código penal (GÓMEZ TOMILLO, M. (dir.)).* Valladolid: Lex Nova.

TONIATTI, R. 1991. Libertad Informática y Derecho a la protección de los datos personales: principios de legislación comparada. *Revista*

Vasca de Administración Pública. Herri-Arduralaritzako Euskal Aldizkaria, 139.

TRAMULLAS SAZ, J. 1997. Los sistemas de información: una reflexión sobre información, sistema y documentación, 7, 1.

TRAPERO BARREALES, M. A. 2006. Los delitos de incendio, estragos y daños tras la reforma de la Ley Orgánica 7/2000 y la Ley Orgánica 15/2003, Valencia, Tirant lo Blanch.

TRENTACAPILLI, D. 2002. Accesso abusivo ad un sistema informatico e adeguatezza delle misure di protezione. *Diritto penale e proceso*, nº 10.

VANNINI, R. 1994. La criminalità informatica: le tipologie di computer crimes di cui alla l. 547/93 dirette alla tutela della riservatezza e del segreto. *Rivista Trimestrale di Diritto Penale e dell'Economia*.

VARGAS PINTO, T. 2007. Delitos de peligro abstracto y resultado Navarra, Thomson Reuters.

VASSILAKI, I. E. 2008. Report- Das 41.StrÄndG-Die neuen strafrechtlichen Regelungen und ihre Wirkung auf die Praxis. *Computer Und Recht: Forum für die Praxis des Rechts der Datenverargeitung, Information und Automation*, 24, 131-136.

VICARIOLI, L. 2008. Manuale Diritto penale Parte Speciale I (ANTOLISEI, FRANCESCO), Mliano, Giuffrè Editore.

VIDAL MARTÍNEZ, J. 1980. Manifestaciones del derecho a la intimidad personal y familiar. *Revista General de Derecho*.

VIDAL MARTÍNEZ, J. 1984. El derecho a la intimidad en la Ley Orgánica de 5 de mayo de 1982, Madrid, Montecorvo.

VITARELLI, T. 2011. Tutela della vita privata. Diritto penale. Parte speciale, Volume I, Tutela penale della persona (PULITANÒ, DOMENICO (dir.)). Torino: Giappichelli.

VIVES ANTÓN, T. S. 1981. La estructura de la teoría del concurso de infracciones, Valencia, Universidad de Valencia.

VIVES ANTÓN, T. S. 1995. *La libertad como pretexto,* Valencia, Tirant lo Blanch.

VON BERTALANFFY, L. 1945. Zu einer allgemeinen Systemlehre. *Blätter für deutsche Philosophie,* 3/4**,** 139-164.

VON BERTALANFFY, L. 1950. An Outline of General System Theory. *British Journal for the Philosophy of Science,* 1**,** 139-164.

VON BERTALANFFY, L. 1951. General system theory - A new approach to unity of science (Symposium). *Human Biology,* 23**,** 303-361.

VON BERTALANFFY, L. 1968. General System theory: Foundations, Development, Applications, New York, George Braziller.

VON BERTALANFFY, L. 1975. Perspectives on General Systems Theory. Scientific-Philosophical Studies, New York, George Braziller.

WEIDEMANN, M. 2010. § 202a. Strafgesetzbuch Kommentar (VON HEINTSCHEL -HEINEGG, BERND). München: Verlag C.H.Beck.

WELZEL: Derecho Penal. Parte General (Traducción de Carlos Fontán Balestra), Buenos Aires: Roque Depalma, 1956.

ZIPF. 1970a. Die Bedeutung und Behandlung der Einwilligung im Strafrecht, Osterrreichische Juristenzeitung,.

ZIPF. 1970b. Einwilligung und Risikoübernahme in Strafrecht, Henwied: Luchterhand.

JURISPRUDENCIA SOBRE ACCESO ILÍCITO

I. ANTERIOR A LA INTRODUCCIÓN DE LA CONDUCTA:

A) DEL TRIBUNAL SUPREMO:

- S. Tribunal Supremo número 358 de 30 abril 2007.

B) JURISPRUDENCIA MENOR:

- S. Juzgado de lo Penal de Barcelona nº 2 de 28 mayo 1999 (caso Hispanack).

- S. Audiencia Provincial de Tarragona número 23 julio 2001.

- A. Juzgado de lo Penal Lorca número 2 de 29 enero 2002.

- S. Audiencia Provincial de Huelva número 76 de 16 junio 2006.

- S. Audiencia Provincial de Córdoba número 297 de 28 noviembre 2008.

II. SOBRE EL ARTÍCULO 197.3 DEL CÓDIGO PENAL:

A) DEL TRIBUNAL SUPREMO:

- S. Tribunal Supremo número 40 de 3 febrero 2016 que casa parcialmente la S. Audiencia Provincial de Baleares (Sección 2ª) número 5 de 28 de enero de 2015.

- S. Tribunal Supremo número 407 de 12 mayo 2016.

B) JURISPRUDENCIA MENOR:

- S. Audiencia Provincial de Valladolid (Sección 4ª) número 102, de 18 de marzo.

- S. Audiencia Provincial de Madrid (Sección 2ª) número 402, de 17 de julio de 2012.

- S. Audiencia Provincial de Álava (Sección 2ª) número 74 de 7 marzo 2013.

- S. Audiencia Provincial de Asturias (Sección 2ª) número 38 de 24 enero 2013.

- S. Audiencia Provincial de Vizcaya (Sección 2ª) número 90307 de 23 julio de 2014.

- S. Audiencia Provincial de Girona (Sección 4ª) número 504 de 22 septiembre 2014.

- S. Audiencia Provincial de Baleares (Sección 2ª) número 5 de 28 enero 2015.

- S. Audiencia Provincial de Madrid (Sección 2ª) número 329, de 27 de abril.

- S. Audiencia Provincial del Murcia (Sección 3ª) número 88 de 20 febrero 2015.

- S. Audiencia Provincial de Girona (Sección 4ª) número 358 de 22 junio 2015.