Circular 3/2017, *sobre la reforma del código penal operada por la LO 1/2015 de 30 de marzo en relación con los delitos de descubrimiento y revelación de secretos y los delitos de daños informáticos*

Introducción

La reforma llevada a efecto en el Código penal por la LO 1/2015, de 30 de marzo, afecta de forma importante a la regulación hasta ahora existente en materia de delitos de descubrimiento y revelación de secretos y de daños informáticos. Los primeros encuadrados en el Capítulo I del Título X del Libro II del CP, dedicado a *"Los delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio"*, y los segundos en el Capítulo IX del Título XIII del Libro II del CP, dedicado a los *"Delitos contra el Patrimonio y contra el Orden Socioeconómico.*

El Preámbulo de la citada Ley Orgánica, en su apartado XIII, se refiere a las modificaciones introducidas en estas tipologías delictivas como consecuencia de la incorporación al ordenamiento jurídico interno de la Directiva 2013/40/UE, del

Parlamento y del Consejo, de 12 de agosto de 2013, relativa a los ataques contra los sistemas de información. Pero las novedades incorporadas en los tipos penales concernientes a los delitos de descubrimiento y revelación de secretos obedecen también a la voluntad del Legislador de ofrecer respuesta penal ante determinados comportamientos, concretamente los relacionados con la divulgación de imágenes o grabaciones de una persona que**,** aun obtenidas con su consentimiento, se difunden contra su voluntad afectando gravemente a su intimidad personal.

En cualquier caso, el análisis de las novedades incorporadas en unos y otros tipos delictivos exige previamente una reflexión sobre el sentido y alcance de la Directiva 2013/40/UE. Al respecto ha de recordarse que dicha norma europea, dictada en el marco del proceso de aproximación de las legislaciones penales de los Estados miembros en que nos encontramos inmersos, sustituye a la Decisión Marco 2005/222/JAI del Consejo, de 24 de febrero de 2005, relativa también a los ataques contra los servicios de información, cuya publicación en febrero del año 2005 tuvo un doble objetivo: por una parte el establecimiento de normas mínimas comunes para todos los Estados en la definición de las infracciones penales para hacer frente a los ataques informáticos y las sanciones aplicables a las mismas, y de otro lado reforzar y mejorar la cooperación entre las autoridades competentes de los Estados y los organismos europeos con responsabilidad en esta materia.

La citada Decisión Marco 2005/222/JAI fue incorporada al ordenamiento jurídico español a través de la reforma operada en el Código Penal por Ley Orgánica 5/2010, de 22 de junio, que dio lugar a la modificación del art. 197 del Código Penal y concretamente a la tipificación del acceso ilegal a sistemas informáticos, en el apartado tercero del citado precepto, así como a la previsión, en el párrafo segundo de este mismo apartado, de las penas correspondientes a las personas jurídicas en los supuestos en que resultaran responsables de estos ilícitos en aplicación del art. 31bis del mismo texto legal. También fruto de este mismo objetivo, de incorporación al ordenamiento interno de la citada norma europea, se añadió en éste mismo precepto un nuevo apartado, el número 8, en el que se contemplaba

una agravación de la pena cuando los delitos hubieran sido cometidos en el seno de una organización o grupo criminal.

Asimismo, la transposición de la indicada Decisión Marco dio lugar a la tipificación específica en el art. 264 CP de los delitos de daños informáticos, en relación con los cuales también se contempló, siguiendo las directrices de dicha norma europea, similar agravación penológica en los supuestos de actuación en el marco de una organización criminal, así como la posibilidad de extender la responsabilidad penal por estos hechos a las personas jurídicas cuando concurrieran las circunstancias previstas en el art. 31 bis CP, estableciéndose en el apartado 4º citado precepto, las sanciones imponibles en esos supuestos.

Pese a este esfuerzo realizado por el Legislador, tanto español como europeo, por definir los tipos delictivos que permitieran la persecución y sanción en vía penal de determinados comportamientos surgidos al hilo del desarrollo tecnológico cuyo objeto son los propios datos y sistemas informáticos, la rápida evolución de esas mismas tecnologías ha ido determinando, en pocos años, la aparición de nuevos riesgos y amenazas y, por ende, la necesidad de articular otras figuras delictivas -o modificar las ya existentes- de tal forma que sea posible actuar penalmente frente a estas nuevas situaciones cuando se estime que por su gravedad y por los riesgos que generan se hacen acreedoras de dicho reproche.

Se refiere concretamente la Directiva a la amenaza que supone para la Unión el riesgo de ataques informáticos de carácter terrorista o de naturaleza política contra los sistemas informáticos de las infraestructuras críticas de los Estados Miembros o de las Instituciones de la Unión, e igualmente a la tendencia creciente hacia ataques a gran escala a partir de nuevos métodos de actuación como la creación y utilización de redes infectadas de ordenadores (*botnets*). Por ello el Legislador europeo plantea la necesidad de dotarse de herramientas legales que permitan hacer frente a determinadas conductas, particularmente aquellas que se producen en fases más incipientes de la planificación y desarrollo de la actividad delictiva, así

como el establecimiento de sanciones más graves en atención a la importancia o trascendencia de los sistemas afectados por los ciberataques.

De acuerdo con este planteamiento, la Directiva 2013/40/UE insta a los Estados a la tipificación penal de nuevas conductas no contempladas en la Decisión Marco 2005/222/JAI tales como la interceptación ilegal de transmisiones no públicas de datos informáticos o la producción intencional, venta, adquisición para el uso, importación, distribución u otra forma de puesta a disposición de instrumentos aptos para cometer este tipo de infracciones con la intención de que sean utilizados con esa finalidad. La Directiva también demanda de los Estados el establecimiento para esta clase de ilícitos de penas efectivas, proporcionadas y disuasorias, contemplando agravaciones en atención a circunstancias tales como la importancia de los daños causados, la afectación de sistemas de infraestructuras críticas o la utilización en la acción criminal de datos de carácter personal de otra persona.

No sería completa esta introducción sin reseñar que esta Directiva europea toma como punto de partida para la definición de los tipos penales los arts. 2 a 6 de la Convención sobre Ciberdelincuencia -también conocida como Convención de Budapest-, aprobada por el Consejo de Europa en el año 2001 y ratificada por España en Instrumento publicado en el BOE el 17 de septiembre de 2010. Ello se debe a que el Consejo Europeo, en Conclusiones adoptadas en noviembre del año 2008, consideró que cualquier estrategia de actuación sobre esta materia en el ámbito de la Unión Europea debía tener como marco jurídico de referencia la citada Convención del Consejo de Europa. Consecuentemente, la Directiva no solamente asume sus directrices en las definiciones que incorpora en su articulado sino que, en su considerando decimoquinto, también insta a los Estados Miembros que aún no lo hayan hecho a llevar a efecto el proceso de ratificación de la misma.

Esta decisión se enmarca en el objetivo -plenamente aceptado en la Unión Europea, y en menor medida en otros espacios geográficos más amplios- de hacer posible un uso seguro del ciberespacio en el que se garanticen los derechos de

todos los ciudadanos y también la protección de organismos e instituciones públicos y privados y de los propios Estados. Se trata de un planteamiento abierto que pretende alcanzar a cualquier actividad que se desarrolle a través de las redes y que ha dado lugar, entre otras iniciativas, a la elaboración de una Estrategia Europea de Ciberseguridad, a la aprobación en diciembre del año 2013 de nuestra propia Estrategia de Ciberseguridad Nacional y más recientemente a la tramitación y publicación de la Directiva (UE) 2016/1148, de 6 de julio, sobre seguridad de las redes y de la Información, destinada a armonizar y coordinar las actuaciones de los Estados de la Unión frente al desafío que supone ofrecer respuestas eficaces contra el uso irregular del ciberespacio, una de cuyas manifestaciones más perversas es precisamente la cibercriminalidad.

1. Novedades introducidas en los delitos de descubrimiento y revelación de secretos

Las modificaciones operadas en estos delitos proceden de dos momentos distintos en la tramitación parlamentaria del proyecto de ley de reforma del CP. En un primer momento las modificaciones se limitaban a la incorporación, en un apartado (4 bis) del art. 197, de un nuevo tipo penal para sancionar las conductas de quienes sin autorización de la persona afectada difundieran o revelaran a terceros imágenes o grabaciones de carácter privado obtenidas con la anuencia de aquella cuando dicha divulgación supusiera un grave menoscabo en su intimidad y, por otro lado, a efectuar una pequeña modificación de carácter sistemático, en el apartado 7 del citado precepto.

Sin embargo, la publicación de la Directiva 2013/40/UE de 12 de agosto, antes referida, determinó la introducción, ya en trámite parlamentario, de las novedades que tienen por objeto incorporar en nuestro ordenamiento jurídico dicha Directiva, cuyo plazo de implementación finalizaba en septiembre del año 2015. A dicho fin

no solo se modifica el actual art. 197 CP sino que se añaden los artículos 197 bis, ter, quater y quinquies.

1.1 Nueva redacción del art. 197 CP.

Las novedades en el art. 197 son las siguientes:

A) El delito de acceso ilegal a sistemas informáticos, tipificado hasta el momento, y desde la reforma operada en el Código Penal por Ley Orgánica 5/2010, de 22 de junio, en el apartado tercero de este precepto, se traslada al nuevo art. 197 bis, lo que determina la reordenación de los apartados 4, 5, 6 y 7 del anterior art. 197 que en su vigente redacción pasan respectivamente a reenumerarse como 3, 4, 5 y 6.

Según se hace constar en el Preámbulo, siguiendo con ello el propio planteamiento de la Directiva europea, *se introduce una separación nítida entre los supuestos de revelación de datos que afectan directamente a la intimidad personal y el acceso a otros datos o informaciones que pueden afectar a la privacidad pero que no están referidos directamente a la intimidad personal; no es lo mismo el acceso al listado personal de contactos que recabar datos relativos a la versión del software empleado o a la situación de los puertos de entrada a un sistema. Por ello se opta por una tipificación separada y diferenciada del mero acceso a los sistemas informáticos.*

La decisión de sancionar separadamente el acceso ilegal a sistemas, adoptada por el Legislador ha de considerarse acertada, ya que su anterior ubicación resultaba perturbadora en la interpretación y aplicación de este tipo penal. Es evidente que en éstos casos el bien jurídico protegido, no es directamente la intimidad personal, sino más bien la seguridad de los sistemas de información en cuanto medida de protección del ámbito de privacidad reservado a la posibilidad de conocimiento público. Lo que sanciona este precepto es el mero acceso a un sistema vulnerando las medidas de seguridad y sin estar autorizado para ello, sin que se exija que

dicha conducta permita, de lugar, o posibilite en alguna forma el conocimiento de información de carácter íntimo o reservado. Con la tipificación en un precepto independiente se solventa la incongruencia, denunciada por buena parte de la doctrina, de sancionar esta conducta en el marco de un tipo penal definido por el dolo específico de *descubrir los secretos o vulnerar la intimidad de otro.*

B) El antiguo apartado quinto de este precepto, además de su reordenación numérica como apartado cuarto a la que anteriormente se ha hecho referencia, es objeto de modificación al incorporar una nueva circunstancia determinante de la elevación de la pena privativa de libertad que será, de concurrir la misma, la de tres a cinco años. Así, junto a la tradicional agravación prevista para los supuestos en que los autores del hecho ilícito sean las personas encargadas o responsables de los ficheros, soportes informáticos, electrónicos o telemáticos, archivos o registros, se contempla en el nuevo texto, con igual carácter, el supuesto en que los hechos sancionados en los párrafos 1º y 2º del mismo artículo *se lleven a cabo mediante la utilización no autorizada de datos personales de la víctima.*

Lo que el Legislador pretende sancionar más gravemente son aquellas conductas en las que el autor del hecho no solo invade intencionadamente la intimidad de una persona, cometiendo alguna de las conductas típicas, sino que además lleva a efecto dicho comportamiento haciendo uso de las señas de identidad propias de la víctima, es decir, haciéndose pasar por ella como medio para lograr sus criminales propósitos. Esta agravación, aunque está contemplada para su apreciación en cualquiera de las acciones previstas en los apartados 1 y 2 del art. 197 CP, encuentra su pleno significado en las conductas de acceso, apoderamiento o modificación de información de carácter personal almacenada en archivos o registros públicos o privados, para cuya ejecución suele resultar necesario acreditar que quien actúa es el titular de la información, bien sea ante terceros encargados de su custodia bien sea para superar las barreras tecnológicas establecidas como medio de asegurar esa protección. De hecho, en este último caso, la agravación

concurrirá en muchos de los supuestos, por la necesidad de hacer uso de contraseñas personales para el acceso a dichos registros o archivos.

Como ya se ha indicado, el precepto se refiere a los supuestos de utilización de datos personales. Como tales han de entenderse no solo los datos de identidad oficial, en sentido estricto, sino cualesquiera que sean propios de una persona o utilizados por ella y que la identifiquen o hagan posible esa identificación frente a terceros tanto en un entorno físico como virtual. A los efectos de integrar este concepto, el art. 3 a) de la Ley Orgánica de Protección de Datos 15/1999, de 13 de diciembre, define los datos de carácter personal como *cualquier información concerniente a personas físicas identificadas o identificables*, definición que se complementa con el art. 5.1 f) del Reglamento que desarrolla tal Ley Orgánica, aprobado por Real Decreto 1720/2007, de 21 de diciembre, que entiende por tales *cualquier información numérica, alfabética, gráfica, fotográfica, acústica o de cualquier tipo concerniente a personas físicas identificadas o identificables.* El mismo Reglamento proporciona en el apartado 5.1 o) el concepto de persona identificable describiéndola como *toda persona cuya identidad pueda determinarse directa o indirectamente, mediante cualquier información referida a su identidad física, fisiológica, psíquica, económica, cultural o social. Una persona física no se considerará identificable si dicha identificación requiere plazos o actividades desproporcionados.*

La Directiva 95/46/CE del Parlamento y del Consejo, de 24 de octubre, relativa a la protección de las personas físicas en lo que respecta al tratamiento de los datos personales y a la libre circulación de los mismos, definía los datos personales en su art. 2 a) como *toda información sobre una persona física identificada o identificable. Se considerará identificable toda persona cuya identidad pueda determinarse directa o indirectamente, en particular mediante un número de identificación o uno o varios elementos específicos característicos de su identidad física, fisiológica, psíquica, económica, cultural o social.*

Actualmente, el nuevo Reglamento (UE) sobre Protección de Datos, 679/2016 del Parlamento y del Consejo de 27 de abril, que deroga la Directiva antes mencionada y que será aplicable a partir del 25 de mayo de 2018, precisa aún más el alcance del concepto al considerar datos personales, en su art. 4.1), *toda información sobre una persona física identificada o identificable (el interesado)*, indicando a continuación que *se considerará persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo, un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona.*

En consecuencia no solo cabría entender como tales el nombre y apellidos sino también, entre otros, los números de identificación personal como el correspondiente al DNI, el número de teléfono asociado a un concreto titular (Informe Agencia Española de Protección de Datos nº 285/2006), el número de afiliación a la Seguridad Social o a cualquier institución u organismo público o privado, la dirección postal, el apartado de correos, la dirección de correo electrónico (apartado II recomendación (R99) 5 de 23 de febrero del Consejo de Europa), la dirección IP (STS Sala 3ª de 3 de octubre de 2014, recurso nº 6153/2011; SSTS de la Sala 2ª nº 16/2014 de 30 enero y 167/2016 de 2 de marzo, entre otras, y STJUE de 19 de octubre 2016 asunto Patrick Breyer contra Alemania) la contraseña/usuario de carácter personal, la matrícula del propio vehículo (Informe Agencia Española de Protección de Datos nº 425/2006), las imágenes de una persona obtenidas por videovigilancia (Dictamen 4/2007 del Grupo de Trabajo creado al amparo del art. 29 de la Directiva 95/46/CE), los datos biométricos y datos de ADN (Dictamen 4/2007 citado), los seudónimos (Dictamen 4/2007 citado) los datos personales relativos a la salud física o mental de una persona (art 4 del Reglamento europeo sobre Protección de Datos) así como también los datos identificativos que el afectado utilice habitualmente y por los que sea conocido.

C) Se suprime el apartado 8 del vigente art. 197 referido en su versión anterior a los supuestos en que los hechos se cometan en el seno de una organización o grupo criminal, pasando a integrar dicha circunstancia el nuevo art. 197 quater.

D) Se incorpora un nuevo apartado séptimo al art. 197 cuyo alcance y contenido se analiza a continuación.

1.2 El nuevo apartado 7º del art. 197 CP

La redacción de este nuevo apartado es la siguiente:

Será castigado con una pena de prisión de tres meses a un año o multa de seis a doce meses el que, sin autorización de la persona afectada, difunda, revele o ceda a terceros imágenes o grabaciones audiovisuales de aquélla que hubiera obtenido con su anuencia en un domicilio o en cualquier otro lugar fuera del alcance de la mirada de terceros, cuando la divulgación menoscabe gravemente la intimidad personal de esa persona.

La pena se impondrá en su mitad superior cuando los hechos hubieran sido cometidos por el cónyuge o por persona que esté o haya estado unida a él por análoga relación de afectividad, aun sin convivencia, la víctima fuera menor de edad o una persona con discapacidad necesitada de especial protección, o los hechos se hubieran cometido con una finalidad lucrativa.

Es este un precepto con el que el Legislador pretende hacer posible la respuesta penal ante determinadas conductas asociadas con frecuencia, aunque no necesariamente, a supuestos de ruptura en relaciones de pareja o de amistad, que se ven favorecidas por la potencialidad que ofrecen las tecnologías de la información y la comunicación (en adelante TIC) para el copiado y difusión de imágenes y contenidos. Este tipo de conductas, que se están detectando con

relativa frecuencia, resultaban hasta ahora difícilmente encuadrables en el art. 197 CP en su redacción previa a la reforma analizada, porque el tipo penal exigía que las imágenes o grabaciones audiovisuales que posteriormente iban a difundirse se hubieran obtenido sin consentimiento de la persona cuya intimidad resulta vulnerada. Por el contrario, lo que caracteriza a los supuestos que nos ocupan es que las imágenes/grabaciones se obtienen con la anuencia de la persona afectada, sobre la base, generalmente, de una relación de confianza, disponiéndose después de ellas, en perjuicio de la víctima, muchas veces por motivos de venganza o despecho.

Por eso, hasta el momento, la única posibilidad de actuar penalmente frente a estos comportamientos -y así lo ha venido haciendo el Ministerio Fiscal- era por la vía del art. 173.1 del CP, y aun así, solo cuando resultaba posible acreditar que la difusión pública de imágenes o grabaciones de la víctima suponía un menoscabo en su integridad moral.

El nuevo tipo penal se refiere específicamente a imágenes o grabaciones audiovisuales de otra persona. Por tales hay que entender tanto los contenidos perceptibles únicamente por la vista, como los que se captan conjuntamente por el oído y la vista y también aquellos otros que, aun no mediando imágenes, pueden percibirse por el sentido auditivo. El Legislador no excluye ninguno de estos supuestos y ciertamente la difusión inconsentida de contenidos, en cualquiera de estas formas, es susceptible de determinar un menoscabo en la intimidad del afectado.

Para que el precepto sea aplicable es necesario que la grabación objeto de difusión se haya llevado a efecto en un marco espacial de carácter reservado, circunstancia ésta que el tipo penal concreta en la exigencia de que se haya obtenido en un domicilio, o en un lugar fuera del alcance de la mirada de terceros, y con consentimiento o anuencia del afectado por ello. Es decir, resulta esencial a efectos de asegurar el carácter íntimo de la imagen o grabación, el lugar de la realización o

toma de la misma, que ha de tratarse de un espacio físico excluido, en ese momento, al conocimiento de terceros.

La interpretación del concepto de domicilio, a estos efectos, no ofrece dificultad y ha sido objeto de una copiosa y pacífica elaboración jurisprudencial, que resume la STS nº 731/2013 de 7 de octubre, con cita de otras muchas, al indicar que *este concepto ha de entenderse de modo amplio y flexible ya que trata de defender los ámbitos en que se desarrolla la vida privada de la persona, debiendo interpretarse a la luz de los principios que tienden a extender al máximo la protección a la dignidad, a la intimidad de la persona y al desarrollo de su privacidad a través de la cual proyecta su "yo anímico" en múltiples direcciones*. Entendido en este contexto, el domicilio es *el reducto último de la intimidad personal y familiar* (SSTC nº 69/1999 de 26 de abril y 283/2000 de 27 de noviembre, entre otras); y, a tal fin es indiferente que se trate del correspondiente a la víctima, al agresor o a un tercero.

Más dificultades ofrece, dada su imprecisión, la expresión *otro lugar fuera del alcance de la mirada de terceros* que puede generar problemas importantes a efectos probatorios. En teoría podría incluirse en esta expresión cualquier lugar cerrado, como un local comercial no abierto al público, o también un lugar al aire libre, si bien en este caso habría que acreditar que reúne garantías suficientes de privacidad de tal forma que pueda asegurarse que las escenas/imágenes, captadas o grabadas, lo fueron en un contexto de estricta intimidad y sustraído a la percepción de terceros ajenos a ellas. En ese sentido el concepto *tercero*s habría que entenderlo referido a personas ajenas al acto o situación objeto de grabación, pues es obvio que en dichos acontecimientos pueden intervenir más de una persona y resultaría incongruente entender que el precepto es de aplicación únicamente en los supuestos en que en las escenas objeto de captación intervienen exclusivamente la víctima y quien después dispone de ellas.

En definitiva, lo que el Legislador parece que ha pretendido con esta expresión es dejar constancia de que las imágenes que posteriormente se difunden tenían, en su

origen, un carácter estrictamente privado -aunque no necesariamente con connotaciones sexuales- y que por las condiciones en que se obtuvieron -con anuencia de la víctima-, de no haber infringido el responsable criminal el deber/compromiso de sigilo o confidencialidad contraído implícitamente con la víctima, dicho carácter estaba asegurado. El problema, no obstante, es que la fórmula empleada por el Legislador para definir esta situación de privacidad o intimidad resulta en sí misma excesivamente cerrada y puede plantear dificultades prácticas en orden a su acreditación.

La conducta típica consiste en difundir, revelar o ceder a terceros las referidas imágenes sin la autorización de la persona afectada. La falta de autorización de la víctima habrá de ser valorada en cada supuesto concreto de acuerdo con las circunstancias concurrentes. A estos efectos la declaración de la víctima constituirá, sin duda, un elemento esencial. En cualquier caso no resultará necesario acreditar una negativa expresa sino que podrá ser bastante con la no constancia de autorización, situación a la que han de equipararse los supuestos de falta de conocimiento por parte del afectado de la ulterior cesión o distribución.

Por terceros, como se ha expuesto, habrá que entender aquellas personas ajenas al círculo íntimo en el que se han obtenido las imágenes. Por su parte, personas afectadas serán aquella o aquellas cuya intimidad se vea menoscabada por la cesión o distribución inconsentida de las imágenes que protagonizan o en las que se encuentran reflejadas. Si las personas que aparecen en las imágenes fueran varias la difusión solo sería atípica si hubieran accedido a la misma todas y cada una de las personas que figuran en la imagen o grabación. No obstante a esos efectos ha de tenerse en cuenta que se trata de un delito únicamente perseguible a instancia del agraviado o de su representante legal, tal y como establece el art. 201 CP, por lo que únicamente

podría denunciar el hecho quien no habiendo autorizado la distribución se hubiera visto perjudicado por la misma.

No resulta ocioso recordar que nos hallamos ante un delito semipúblico en el que, por mor de lo dispuesto en el apartado tercero del citado artículo 201 CP, el perdón del ofendido o su representante legal *extingue la acción penal sin perjuicio de lo dispuesto en el segundo párrafo del número 5º del apartado 1º del artículo 130 del mismo texto legal,* relativo éste último a los supuestos de menores o personas con discapacidad necesitadas de especial protección. En consecuencia, el perdón de la persona cuya imagen hubiera sido difundida sin su autorización, producirá el indicado efecto cuando haya sido prestado en forma libre y voluntaria, circunstancia que habrán de valorar los Fiscales en cada caso concreto y en atención a las circunstancias concurrentes, especialmente en los supuestos -desgraciadamente frecuentes- en los que la conducta prevista en el artículo 197-7, se relaciona con situaciones de violencia de género y/o violencia doméstica.

Dadas las posibilidades que ofrecen las nuevas tecnologías de reenvío en forma casi instantánea de imágenes o grabaciones a un número ilimitado de personas -de lo que el llamado *retuiteo* es un excelente ejemplo-, necesariamente debe plantearse si el responsable criminal de esta conducta sería solo quien habiendo obtenido directamente la imagen íntima la difunde después, sin contar con la autorización de la víctima, o también todos aquellos que habiendo recibido dicha imagen/grabación como consecuencia del primer envío, o de una sucesión de ellos, la distribuyen a su vez a otras personas. Teniendo en cuenta la redacción del precepto, es claro que el tipo penal del artículo 197.7 se ha configurado como un delito especial propio del que únicamente serían autores aquel o aquellos que, habiendo obtenido con la anuencia de la víctima la imagen o grabación comprometida inician, sin autorización del afectado, la cadena de difusión cediendo o distribuyendo dichos

contenidos íntimos a otros, ajenos inicialmente -*extranei*-, a esa inicial relación con la víctima y a la obtención, por tanto, de la imagen o grabación comprometida. Ciertamente, en la conducta ilícita que examinamos pueden concurrir las diferentes formas de participación que contemplan los artículos 28 y 29 CP. Así, cabría la coautoría cuando dos o más personas comparten el dominio del hecho y obtienen las imágenes que posteriormente y sin autorización distribuyen, y la cooperación necesaria y la inducción en quienes, sin haber intervenido en la obtención de la imagen y antes de inicial transmisión, inducen o cooperan con los autores en la divulgación o cesión de los contenidos a otras personas. Es igualmente factible la participación como cómplice por parte de quien, sin estar incluido en los anteriores supuestos, colabora en la ejecución del hecho con actos anteriores o simultáneos.

Cuestión distinta es la actuación de los terceros -*extranei*- que sin haber intervenido en la acción inicial antes descrita reciben en un momento posterior los contenidos comprometidos y los transmiten a otras personas distintas, conductas estas que, por mor de las posibilidades que ofrecen las herramientas tecnológicas, pueden reiterarse indefinidamente por una pluralidad de personas. Dichos comportamientos, en principio, únicamente podrían dar lugar a la utilización de los mecanismos previstos en la L.O 1/1982 del protección civil del derecho al honor, a la Intimidad personal y familiar y a la propia imagen.

No obstante, en referencia a estos últimos comportamientos, habría de valorarse la posibilidad de apreciar la comisión de un delito contra la integridad moral del artículo 173.1 CP respecto de aquellos que, siendo *extranei* a la conducta del artículo 197.7, realizan ulteriores transmisiones a terceros de los contenidos comprometidos, a sabiendas de que la difusión se está llevando a efecto sin contar con la autorización del afectado y que la misma, en atención a la especial naturaleza de los contenidos y a las circunstancia concurrentes, puede menoscabar gravemente su integridad moral.

Esta misma posibilidad podría también ser tenida en cuenta respecto del propio autor de la conducta que es objeto de examen en aquellos supuestos en que la difusión inconsentida lesione no solo la intimidad del afectado sino que también, por la naturaleza de las imágenes difundidas, produzca una grave afección en la integridad moral de la persona concernida. En estos supuestos, al resultar afectados bienes jurídicos distintos, se produciría un concurso ideal entre el delito contra la intimidad del artículo 197.7 y un delito contra la integridad moral del artículo 173.1, ambos del CP a penar de conformidad con el artículo 77.2 del mismo texto legal.

El tipo penal exige que la divulgación *menoscabe gravemente la intimidad personal* del afectado. Es este un elemento que habrá de valorarse caso a caso, en atención a las circunstancias concurrentes, es decir, a partir del contenido mismo de la grabación, de la situación y condiciones en la que se llevó a efecto, e incluso de las propias características personales de la víctima. En realidad es un factor que, en alguna forma, impregna toda la interpretación del delito analizado, pues para que la acción sea típica será necesario que la imagen o grabación tenga una naturaleza esencialmente reservada, también que se haya tomado en un marco estrictamente privado y que su difusión pueda provocar una seria injerencia en el ámbito personal de intimidad del afectado, porque solo en ese caso el conocimiento por terceros de dichos contenidos podría generar una grave afección en su derecho a la intimidad personal. Al respecto es interesante recordar que, aun cuando normalmente las imágenes o grabaciones tendrán carácter sexual, las mismas pueden reflejar otros aspectos de la intimidad, tales como las creencias, la ideología, la salud física o psíquica o la situación económica del perjudicado.

Finalmente debe recordarse que el Legislador ha previsto la imposición de la pena en su mitad superior en los tres supuestos que se relacionan en el párrafo segundo de este artículo:

a) Cuando el responsable fuera el cónyuge o la persona que esté, o haya estado unida a él (a la víctima), por análoga relación de afectividad, aun sin convivencia.
b) Cuando la víctima fuera un menor o una persona con discapacidad necesitada de especial protección.
c) Cuando los hechos se hubieran cometido con finalidad lucrativa.

A propósito de la segunda de estas circunstancias ha de plantearse la concurrencia de este ilícito con los delitos sancionados en el art. 189 CP cuando las imágenes obtenidas y posteriormente difundidas merezcan la consideración de material pornográfico, de conformidad con lo dispuesto en el citado precepto en su actual redacción, concepto en cuya interpretación habrá de tenerse en cuenta lo establecido en la Circular 2/2015 de la Fiscalía General del Estado *sobre los delitos de pornografía infantil tras la reforma operada por LO 1/2015.*

En estos supuestos se produciría un concurso ideal entre el delito que se examina, art. 197.7, párrafo 2º y el art. 189.1º b) ambos del CP, a penar de conformidad con el art. 77.2 del mismo texto legal dado que, como bien se explicaba en la Consulta 3/2006 de la Fiscalía General del Estado, la acción ilícita, no solamente lesiona la intimidad del afectado, cuya imagen se difunde sin su autorización, sino que pone también en peligro la indemnidad sexual de los menores, genéricamente considerados, como bien jurídico protegido en los delitos de pornografía infantil.

1.3 El nuevo art. 197 bis CP

La Ley Orgánica 1/2015 incorpora este nuevo precepto que a su vez tiene dos apartados que recogen respectivamente el acceso ilegal a sistemas informáticos y la interceptación ilegal de datos informáticos.

1.3.1 Acceso ilegal a sistemas informáticos (art. 197 bis.1)

En este precepto se reubica el tipo penal previsto, hasta dicha reforma, en el art. 197.3, que sanciona el acceso ilegal a sistemas de información, también conocido como allanamiento o intrusismo informático, y que fue incorporado por primera vez en nuestra legislación por LO 5/2010, de 22 de junio.

El precepto, aun conservando básicamente su contenido inicial, es objeto de una nueva redacción: *el que por cualquier medio o procedimiento, vulnerando las medidas de seguridad establecidas para impedirlo, y sin estar debidamente autorizado, acceda o facilite a otro el acceso al conjunto o una parte de un sistema de información o se mantenga en él en contra de la voluntad de quien tenga el legítimo derecho a excluirlo, será castigado con pena de prisión de seis meses a dos años.*

Ya se ha indicado anteriormente que, como destaca el Preámbulo de la Ley Orgánica 1/2015, la tipificación independiente de esta figura pretende establecer una clara separación de los supuestos a los que se refiere el art. 197 CP, de acceso, apoderamiento o conocimiento irregular de datos o informaciones que afectan a la intimidad personal, frente a aquellos otros comportamientos en los que, aun existiendo un intromisión ilegal en datos o sistemas ajenos, no se ven afectados los datos de carácter personal o la intimidad de otro de manera directa

La actual redacción del artículo, siguiendo los parámetros de la Directiva 40/2013/UE, mantiene la exigencia para la tipicidad de la conducta de que el acceso se lleve a efecto sin autorización y vulnerando las medidas de seguridad establecidas para impedirlo, y ello pese a que la necesaria confluencia de ambas circunstancias pudiera considerarse redundante. Lo que el Legislador castiga es el acceso no autorizado que se lleva a efecto desplegando una especial energía criminal, pues la aplicación del tipo requiere el quebrantamiento de medidas o

códigos de seguridad, resultando atípica la intrusión no autorizada en la que no concurra dicha circunstancia.

No obstante esta doble exigencia puede ser útil para solventar las dudas que pudieran generarse en determinados supuestos. Efectivamente, en relación con esta conducta y también con las que se sancionan en el nuevo art. 197 ter, los considerandos 16 y 17 de la Directiva 2013/40/UE destacan especialmente la necesidad de constatar que la actividad se realiza con propósito delictivo, indicando al respecto que deberían quedar al margen de una posible responsabilidad penal aquellos supuestos en que la persona desconocía que el acceso no estaba autorizado o cuando, en el marco de una relación laboral o contractual, la conducta observada únicamente supone la infracción de políticas de usuario o el incumplimiento de las normas organizativas sobre utilización de los sistemas de información de la empresa. De acuerdo con este mismo planteamiento el art. 3 de la Directiva, en el que se define la figura que inspira la que nos ocupa, exige expresamente que el comportamiento, para ser susceptible de sanción penal, *haya sido realizado intencionalmente*. Por ello la necesidad de que, además de la ausencia de autorización, sean vulneradas medidas de seguridad para que el acceso pueda considerarse delictivo, minimiza de forma importante las dudas que pudieran generarse en cuanto a la intencionalidad de la conducta.

A tales efectos, tendrá la consideración de medida de seguridad toda aquella que se haya establecido con la finalidad de impedir el acceso al sistema, con independencia de que la misma sea más o menos sólida, compleja o robusta y también de que haya sido establecida por el administrador, el usuario, o por el instalador del sistema, siempre que se mantenga operativa como tal medida de seguridad por quien está legitimado para evitar el acceso.

En cuanto a lo que haya de entenderse por actuar sin autorización, resulta procedente recordar la definición que sobre ello ofrece el art. 2d) de la Directiva 2013/40/UE que entiende como tal aquel *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

En relación con este punto, no debe olvidarse que, en ocasiones, estas conductas pueden llevarse a efecto por los propios encargados/responsables de los sistemas informáticos cuando acceden, intencionadamente y superando barreras de seguridad, a *una parte* del sistema a la que no se extiende su autorización personal. En estos supuestos podría ser eventualmente aplicable la circunstancia genérica de agravación de abuso de confianza del art 22-6º del C. Penal si la vulneración de las medidas de seguridad se ve facilitada por la propia posición privilegiada que ocupa el agente como usuario del sistema atacado.

Sin perjuicio de alguna variación de carácter gramatical las novedades que se introducen en el precepto son esencialmente dos:

a) Se contempla como conducta típica, además del propio acceso a un sistema informático ajeno -en las condiciones mencionadas-, la conducta de facilitar a otra persona ese mismo acceso, en idénticas condiciones, lo que permite incluir en el tipo supuestos no previstos hasta ahora, aunque, al menos en algunos casos, podrían haber sido abarcados como formas de participación criminal.

b) El objeto de la conducta típica se concreta en el *conjunto o una parte de un sistema de información,* suprimiéndose la referencia del precepto, en su inicial redacción, a los datos o programas informáticos contenidos en el sistema al que se accede. Obviamente, la acción de intromisión ilegal en un sistema de información pone al alcance del invasor todo su contenido, datos, programas o cualesquiera otros elementos, por lo que la supresión de la referencia a datos o programas amplía el alcance del precepto abarcando incluso aquellos accesos que alcanzan únicamente a archivos de mera configuración del sistema. Por tanto, con la nueva redacción se evidencia que no es necesario tomar contacto

con datos o programas que contengan informaciones concretas sino que la conducta se consuma con la simple entrada en el sistema o parte del mismo.

Ha de recordarse que la Directiva 2013/40/UE, en su art. 2, define *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*. Al respecto, y para percibir el sentido último del precepto analizado, no ha de olvidarse que la evolución tecnológica ha determinado que existan en nuestros domicilios auténticas redes informáticas domésticas cuyo punto de acceso y comunicación al exterior se lleva a efecto a través de los routers de las operadoras de comunicación. En consecuencia, el acceso a un router -en tanto forma parte de un sistema de información-, vulnerando su contraseña de seguridad, entendida en el sentido antes indicado, podría integrar este delito.

En la práctica será frecuente la concurrencia de este tipo, acceso ilegal a sistemas, con cualquiera de las conductas previstas en el artículo 197 nº 1 y 2, particularmente en los supuestos del párrafo segundo consistentes en el acceso a datos registrados en ficheros o soportes informáticos, electrónicos o telemáticos, pues habitualmente estos registros se encuentran protegidos para el acceso directo por medidas de seguridad. En estos casos, la solución habrá de venir por la apreciación, en términos generales, de un concurso medial del artículo 77 del CP, como igualmente se produciría en el caso, por ejemplo, de que acceso ilegal tuviera por objeto el descubrimiento de secretos de empresa (art 278 CP) o el descubrimiento de secretos oficiales (art. 598 y ss CP). La razón de ello hay que buscarla en la circunstancia de que el acceso ilegal a un sistema informático afecta a bienes jurídicos no exactamente coincidentes con los que son objeto de protección en los otros tipos penales, no siendo además un medio necesario para la ejecución de los delitos previstos en los artículos 197, 1º y 2º; 278 y 598 y ss del CP. Ello no obsta a que, en

supuestos concretos, en los que no sea posible el acceso a la información íntima o a los datos personales por medio distinto a la vulneración de las medidas de seguridad del sistema, pudiera considerarse la posibilidad de apreciar una progresión delictiva que llevaría a considerar el concurso de normas sancionable por la vía del artículo 8.3 CP

En todo caso, cuando para sortear las medidas de seguridad fuera preciso utilizar datos de carácter personal de la víctima, la aplicación del art. 197 bis 1º junto con el artículo 197, 4 b) supondría una infracción del principio *non bis in idem*, debiendo aplicarse en estos casos este último precepto, por mor del principio de especialidad establecido en el artículo 8.1 del CP.

1.3.2 Interceptación ilegal de datos informáticos (art 197 bis.2)

El segundo apartado del nuevo art. 197 bis es un precepto de nuevo cuño que castiga con una pena de prisión de tres meses a dos años o multa de tres a doce meses al *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.*

El primer antecedente de este precepto hay que buscarlo en la Convención sobre Ciberdelincuencia del Consejo de Europa del año 2001 que, en su art. 3, bajo el epígrafe interceptación ilícita, se refiere a estas conductas, en los siguientes términos:

Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno la interceptación deliberada e ilegítima, por medios técnicos, de datos informáticos comunicados en transmisiones no públicas efectuadas a un sistema informático, desde un sistema informático o dentro del mismo, incluidas las emisiones electromagnéticas procedentes de un

sistema informático que contenga dichos datos informáticos. Cualquier Parte podrá exigir que el delito se haya cometido con intención delictiva o en relación con un sistema informático conectado a otro sistema informático.

Por su parte y en términos similares, la Directiva 2013/40/UE del Parlamento Europeo y del Consejo, de 12 de Agosto, recoge esta misma conducta en su art. 6, bajo el subtítulo de interceptación ilegal, en la siguiente forma:

Los Estados miembros adoptarán las medidas necesarias para garantizar que la interceptación, por medios técnicos, de transmisiones no públicas de datos informáticos hacia, desde o dentro de un sistema de información, incluidas las emisiones electromagnéticas de un sistema de información que contenga dichos datos informáticos, intencionalmente y sin autorización, sea sancionable como infracción penal, al menos en los casos que no sean de menor gravedad.

Como se explica en el Preámbulo de la LO 1/2015 la interceptación de comunicaciones personales, salvo en los supuestos de autorización judicial, ya estaba prevista como delito en el art. 197.1 de nuestro CP por lo que, a través de esta reforma y de acuerdo con la Directiva, se sanciona la interceptación no autorizada de cualquier otra transmisión de datos informáticos que no tenga el carácter de comunicación interpersonal y que se lleve a efecto por redes no públicas. Son objeto, por tanto, de protección las comunicaciones entre dos o más sistemas informáticos, las que tienen lugar entre distintos ordenadores dentro de un mismo sistema o incluso las que median entre una persona y un ordenador, como por ejemplo, en palabras del informe preparatorio de la Convención de Budapest, las que se establecen a través del teclado.

El Preámbulo de la LO 1/2015 explica el sentido del precepto haciendo referencia a la interceptación *de transmisiones automáticas -no personales- entre equipos*. Curiosamente el texto del nuevo precepto no recoge el término *automáticas* como calificativo de las transmisiones no públicas de datos que se protegen. Sin embargo

dicho termino es muy clarificador y no ha de perderse de vista para entender que, tras la reforma, la protección penal alcanza también a aquellas transmisiones de datos informáticos que se producen entre sistemas o dispositivos electrónicos al margen de la intervención humana y que tienen su origen en la previa programación o el propio funcionamiento interno del sistema.

Como se constata claramente, el objeto de protección en este tipo penal -y también en los preceptos mencionados que le sirven de antecedente- es doble. En primer término, lo son los datos informáticos que se transmiten entre los distintos dispositivos de un sistema, o entre dos o más sistemas, en forma no pública, es decir aquellos datos que, en atención a su forma de transmisión, quedan excluidos del conocimiento por parte de terceros. Como explica claramente el parágrafo 54 del informe preparatorio de la Convención de Budapest *el término "no públicas" matiza la naturaleza del proceso de transmisión (comunicación) y no la naturaleza de los datos transmitidos. Los datos comunicados pueden ser información que esté accesible al público, pero que las partes quieren comunicar de forma confidencial*.

Habrá que atender por tanto a la forma de transmisión de los datos para concretar la información objeto de protección. Al respecto ha de recordarse que según el Anexo II de la Ley 9/2014, *General de Telecomunicaciones* una red pública de comunicaciones electrónicas es aquella que *se utiliza, en su totalidad o principalmente, para la prestación de servicios de comunicaciones electrónicas disponibles para el público y que soporta la transferencia de señales entre puntos de terminación de la red.* Por el contrario, y según el glosario de la Organización Mundial del Comercio (OMC), una red (privada) no pública es aquella que se utiliza *para establecer comunicaciones dentro de una organización (en contraposición a la prestación de servicios al público) o para suministrar esas comunicaciones a organizaciones basándose en una configuración de instalaciones propias o arrendadas. El término comprende las redes utilizadas por las compañías privadas, las empresas estatales o entidades gubernamentales.*

En este último apartado, por tanto, se han de incluir tanto las redes de área local -denominadas *Local Área Network* (LAN)- que son las que conectan los ordenadores de un área relativamente pequeña y predeterminada, como una habitación, un edificio, o un conjunto de edificios, como las redes locales extensas -conocidas como *Wide Área Network* (WAN)- que conectan varios equipos localizados a una notable distancia entre sí, e incluso pueden conectar varias LAN,s. Pero también han de considerarse como tales las redes privadas de carácter virtual (VPN) que no son sino redes establecidas con garantías de privacidad pero utilizando la infraestructura de la red pública de comunicaciones.

En consecuencia, habrá que considerar amparadas por el precepto que se examina todas las transmisiones efectuadas por redes privadas pero también aquellas que, aun efectuadas a través de redes púbicas, tengan carácter reservado o en relación con las cuales se hayan establecido, de una u otra forma, mecanismos para garantizar la privacidad y excluir a terceros del conocimiento de dicha información.

En segundo término, se protegen también en este precepto los datos informáticos susceptibles de obtenerse a partir de las emisiones electromagnéticas de un sistema de información. Al respecto ha de reseñarse que todos los dispositivos electrónicos, aun estando apagados, emiten continuamente radiaciones a través del aire o de los propios conductores, como lo son los cables que permiten establecer la conexión entre los mismos. La corriente que circula por un conductor genera un campo electromagnético alrededor de éste que es capaz de inducir esta misma señal a otros conductores que estén situados en las proximidades dentro de ese mismo campo. Por ello, si se cuenta con los equipos apropiados, es posible captar estas emisiones y reproducir, a partir de las mismas, información acerca, por ejemplo, de las transmisiones que se están llevando a efecto desde el dispositivo espiado o también de las imágenes que aparecen en la pantalla o de las pulsaciones de su teclado.

El parágrafo 57 del informe antes indicado, previo a la elaboración de la Convención de Budapest, en referencia a este tema indica que las emisiones electromagnéticas no pueden ser consideradas en sí mismas datos informáticos, pero es posible *que los datos puedan ser reconstruidos a partir de dichas emisiones. En consecuencia, la interceptación de los datos provenientes de las emisiones electromagnéticas de un sistema informático está incluida como delito* en el art. 3 de la citada Convención.

La conducta típica sancionada en el art. 197 bis 2º consiste en interceptar las indicadas transmisiones o emisiones electromagnéticas. A qué debe entenderse por interceptación se refiere el considerando 9º de la Directiva 2013/40/UE, según el cual dicho concepto abarca *la obtención del contenido de los datos bien sea directamente, mediante el acceso y recurso a ese sistema de información, o indirectamente, mediante el recurso a sistemas de escucha y grabación electrónicos por medios técnicos.*

En uno y otro caso, para que la conducta sea delictiva, han de concurrir dos requisitos: que quien efectúa la interceptación no esté autorizado para ello y que la misma se realice utilizando como medio *artificios o instrumentos técnicos.* No define más el Legislador, por lo que pueden incluirse como tales artificios o instrumentos cualesquiera herramientas o mecanismos que hagan posible este objetivo aunque no estén específicamente destinados a ello. El Informe previo a la elaboración de la Convención de Budapest, en su parágrafo 53, identifica como medios técnicos los dispositivos que se conectan a las líneas de transmisión y también los dispositivos que pueden utilizarse para obtener y grabar las comunicaciones inalámbricas. Igualmente considera como tales, a dichos efectos, el uso de software, contraseñas y códigos.

Como anteriormente se ha indicado, la ubicación de este delito en el nuevo art. 197 bis. 2º, junto al acceso ilegal a sistemas informáticos, es coherente con la voluntad del Legislador de separar la sanción de las conductas que tutelan la privacidad

protegiendo la seguridad de los sistemas de aquellas otras en las que el bien jurídico protegido es directamente la intimidad de las personas. Las conductas tipificadas en este art. 197 bis 2º no tienen por qué afectar a la intimidad o a los datos de personas concretas y determinadas y si así fuera entrarían en juego las normas concursales. En el supuesto de que la concurrencia se produzca entre la interceptación ilegal del artículo 197 bis 2º y los delitos del artículo 197.1º, el criterio a aplicar será el del concurso de normas a resolver conforme al principio de absorción dado que, como puede observarse, uno de los comportamientos típicos que reseña el último precepto citado es precisamente el de interceptar las comunicaciones o utilizar artificios técnicos de escucha, transmisión, grabación o reproducción de imágenes, sonidos o cualquier otra señal de comunicación, por lo que entraría en juego el artículo 8.3º del CP a cuyo tenor *el precepto legal más amplio o complejo absorberá a los que castiguen las infracciones consumidas en aquel*, siendo de aplicación por tanto el artículo 197.1º.

Ahora bien, en el supuesto de que la interceptación ilegal que estamos examinando (art 197 bis 2º) concurra con alguna de las conductas ilícitas contempladas en el art. 197.2º habrá de apreciarse un concurso medial, del art 77 CP por las mismas razones y con las salvedades expuestas anteriormente en referencia a la concurrencia del artículo 197 bis 1º con esta misma conducta.

1.4 El nuevo art. 197 ter CP

Es este también un precepto de nuevo cuño que trae causa de la Directiva 2013/40/UE que, en su art. 7, insta a la penalización de determinadas acciones relacionadas con los instrumentos destinados a la comisión de determinadas actividades ilícitas en los siguientes términos:

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 arts. 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 arts. 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

También en este caso la Directiva asume el planteamiento de la Convención de Budapest del Consejo de Europa que**,** en su art. 6 y bajo el epígrafe *abuso de los dispositivos*, insta a los Estados-parte a sancionar penalmente este tipo de comportamientos. Lo que en uno y otro caso pretende el Legislador europeo, con la tipificación de estas conductas, es adelantar la barrera de protección penalizando la producción, adquisición o distribución de herramientas e instrumentos preparados y diseñados para cometer las diversas infracciones de acceso ilegal, interceptación ilegal, ataques a los datos y a los sistemas informáticos. La razón de ello hay que buscarla en la preocupación que está generando la tendencia creciente a la planificación y ejecución de ataques a gran escala contra sistemas informáticos. Como se explica en las consideraciones previas de la Directiva esta tendencia coincide y se aprovecha del desarrollo de métodos cada vez más sofisticados, entre ellos y muy particularmente la utilización de redes de ordenadores infectados (*botnets*).

Este tipo de actuaciones se realizan en diversas fases. Así, en primer término, es necesario crear la red de ordenadores a través de los cuales y mediante una acción perfectamente sincronizada sea posible ejecutar un ataque informático masivo. A dicho fin, y utilizando diversas herramientas e instrumentos tecnológicos, se procede a infectar mediante programas nocivos una pluralidad de ordenadores para hacer posible el control remoto de los mismos. Logrado este primer objetivo todos y cada uno de los dispositivos afectados pueden ser activados, sin

conocimiento de su legítimo usuario, y utilizados de forma coordinada en la ejecución de un ataque informático a gran escala contra cualquier sistema de información y causar de esta forma importantes daños a los organismos, instituciones o empresas afectadas.

La Directiva 2013/40/UE llama la atención sobre el extraordinario riesgo que suponen estos *ciberataques a gran escala* dado que pueden producir graves perjuicios económicos, como consecuencia de los daños materiales producidos o de la paralización de actividades o servicios y, también, por la sustracción o destrucción de información sensible o de valor económico reseñable. El peligro que ello supone se entiende fácilmente al considerar la posibilidad de que puedan ser objeto de ese tipo de ataques los sistemas de información de infraestructuras críticas, de entidades u organismos sobre los que se sustenta el desarrollo industrial o empresarial o de las altas Instituciones de los Estados Miembros o de la propia Unión Europea.

En España la preocupación por esta clase de acciones ha quedado reflejada en nuestra Estrategia Nacional de Ciberseguridad que al respecto recuerda que *la multiplicidad de potenciales atacantes incrementa los riesgos y amenazas que pueden poner en graves dificultades los servicios prestados por las Administraciones Públicas, las Infraestructuras Críticas o las actividades de las empresas y ciudadanos. Además, existen evidencias de que determinados países disponen de capacidades militares y de inteligencia para realizar ciberataques que ponen en riesgo la Seguridad Nacional*. Todo ello está determinando algunas iniciativas de interés entre las cuales se encuentra la puesta en marcha por parte del Instituto Nacional de Ciberseguridad (INCIBE) de un Centro Antibotnets que facilita la identificación de ordenadores infectados, informa a los usuarios de esta circunstancia y les proporciona los medios adecuados para hacer posible la desinfección.

Por lo expuesto el Legislador europeo, siguiendo los parámetros de la Convención de Budapest, apuesta por la sanción penal de las fases previas de esta clase de actividades, con la finalidad de conjurar el riesgo que las mismas suponen para el interés general. Pero al hacerlo, definiendo la conductas sancionables en el art. 7 de la Directiva, aplica ese mismo criterio no solo a los instrumentos y herramientas adecuadas para preparar y sustentar ataques masivos sino también a cualesquiera otras aptas para llevar a efecto acciones ilícitas, aun cuando sean de carácter aislado, contra datos o sistemas informáticos.

La LO 1/2015 hace suyo este planteamiento y tipifica estos comportamientos en el CP en relación con dos categorías de delitos. Por una parte en referencia a los daños informáticos, con el contenido y alcance que se analizará en esta misma Circular al estudiar dichas figuras delictivas, cuando el fin pretendido sea el sabotaje informático y de otra parte entre los delitos de descubrimiento y revelación de secretos, cuando el objetivo al que se destinan dichas herramientas sea el espionaje informático. Con esta última finalidad se ha incorporado un nuevo precepto en el Capítulo primero del Título X, el art. 197 ter, con la siguiente redacción:

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 art. 197 o el art. 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.

La conducta típica viene definida por los verbos producir, adquirir para su uso, importar o de cualquier modo facilitar a tercero, las herramientas o instrumentos que se relacionan en los apartados a) y b) del mismo precepto. Por tanto los comportamientos objeto de sanción se encuentran definidos de una forma abierta que incluye tanto la elaboración para uso propio, o para distribución a terceros, como la importación, la adquisición y en consecuencia la ulterior posesión -aunque el precepto no lo diga expresamente, pues tal posesión se habrá alcanzado por alguna de aquellas vías - bien sea para el propio uso o la para distribución o entrega a otro u otros y en general cualquier forma de puesta a disposición de terceros de estos instrumentos/ herramientas. No obstante la posibilidad de actuar penalmente ante dichos comportamientos, se encuentra acotada por dos elementos. El primero de ellos, la falta de autorización para su elaboración, adquisición o facilitación a terceros y el segundo, de carácter teleológico, al exigirse que dichas acciones estén orientadas a *facilitar la comisión de alguno de los delitos a que se refieren los apartados 1 y 2 del art. 197 o el art. 197 bis.*

En realidad ambos elementos son complementarios y responden a una preocupación de la que se deja constancia de forma específica en la propia Directiva europea. Muchas de las herramientas o instrumentos susceptibles de ser empleadas para cometer estos hechos ilícitos pueden haber sido creadas y comercializadas para su uso con objetivos legítimos e incluso necesarios, como los de auditar la seguridad de los sistemas, programas o aplicaciones, detectar vulnerabilidades, garantizar la solidez o fiabilidad de contraseñas o sistemas de seguridad etc. De hecho son numerosas las empresas e instituciones que habitualmente realizan pruebas o ejercicios para analizar las vulnerabilidades de sus sistemas utilizando este tipo de herramientas, y es aconsejable que así se haga pues no en vano uno de los objetivos de la Estrategia Nacional de Ciberseguridad es garantizar un adecuado sistema de seguridad y resiliencia en los sistemas de información de las Administraciones Públicas y en los correspondientes a los organismos y empresas del sector privado.

En consecuencia, para que el hecho sea típico habrán de concurrir las dos circunstancias indicadas. Por una parte que quien así actúa no esté autorizado para ello, bien sea legalmente o porque se le haya encomendado dicha responsabilidad por quien tenga capacidad para ello en el marco concreto de la actividad de que se trate. Pero además ha de actuarse con la finalidad específica de facilitar la comisión de un delito de los indicados en el precepto, circunstancia que habrá de acreditarse en cada supuesto, atendiendo a los elementos, pruebas o indicios existentes.

El Legislador español, en consecuencia, siguiendo la línea de la Directiva, es especialmente riguroso al establecer como requisito para la persecución de estas conductas que los instrumentos o herramientas que relaciona en el precepto se adquieran, posean, importen o distribuyan con la finalidad específica de facilitar la comisión de delitos de descubrimiento o apoderamiento de datos, documentos, mensajes de correo electrónico o efectos personales; interceptación de comunicaciones personales; apoderamiento, utilización o modificación de datos de carácter personal registrados en cualquier tipo de ficheros o soportes; acceso ilegal a sistemas o interceptación de comunicaciones entre sistemas.

Los instrumentos y herramientas objeto de la acción ilícita pueden ser:

1) Programas informáticos concebidos o adaptados principalmente para cometer estos delitos.

Un programa informático o software es un conjunto de instrucciones que una vez ejecutadas realizan una o varias tareas en un ordenador o en un sistema. Según las definiciones que recoge la Directiva 2013/40/UE, los programas informáticos sirven para que el sistema de información realice una función. Dada la forma en que el precepto se refiere a ello, al exigir que sea un programa concebido o adaptado principalmente para cometer un delito, es claro que ha de tratarse de un programa malicioso, diseñado para infiltrarse, obtener información y/o dañar un

dispositivo o un sistema de información sin el consentimiento de su propietario. Según el Instituto Nacional de Ciberseguridad (INCIBE) el software malicioso o *malware* es una amenaza que utiliza múltiples técnicas y vías de entrada: páginas web, correo electrónico, mensajería instantánea, dispositivos de almacenamiento externos (memorias USB, discos duros externos, CDs, DVDs,…), redes P2P, etc. y puertos abiertos en un ordenador. Estas vías, entre otras, son utilizadas por el *malware* para infectar los sistemas informáticos y propagarse por ellos, afectando de distintas formas el uso para el que están destinados (impidiendo acciones, vigilando usos, ralentizando sistemas, ejecutando acciones no permitidas,…).

Entre ellos se encuentran los programas espía *(spyware*) creados con el objetivo de recolectar, sin su conocimiento, información personal de una pluralidad de usuarios o, en su caso, información de interés más general, almacenada en un sistema informático, para enviarla al atacante o a un tercero vía internet con finalidades diversas. Un ejemplo característico de este tipo de malware es el conocido como *ZeuS* utilizado en los ataques de *phishing* bancario y cuyo objeto es el robo de credenciales de usuarios de banca electrónica para su utilización posterior en transacciones fraudulentas. También pueden producir un efecto similar los programas llamados *keyloggers* que registran las pulsaciones en un teclado y de esta forma permiten apoderarse de contraseñas personales.

En otras ocasiones, sin embargo, el programa malicioso está diseñado para un uso más selectivo, orientado a controlar o espiar a personas concretas. Así es conocido -y su uso ha dado lugar a la incoación de diversos procedimientos judiciales- el denominado *cerberus* que, instalado directamente por el agresor en el teléfono móvil de su víctima, hace factible el control y vigilancia de la actividad del terminal y, en consecuencia de la persona afectada, a través del conocimiento de la llamadas entrantes y salientes, la geolocalización del dispositivo e, incluso, la obtención de fotografías o de grabaciones en video y audio realizadas desde la cámara del móvil controlado.

El requisito exigido por el precepto de que se trate de programas *concebidos o adaptados principalmente* para cometer alguno de los delitos sancionados en los apartados 1 y 2 del art. 197 o en el art. 197 bis, con exclusión de otro tipo de programas que no reúnan esta característica aunque puedan ocasionalmente servir para esa misma finalidad, hará necesario generalmente un informe pericial en orden a acreditar esta circunstancia.

2) Contraseñas de ordenador, código de acceso o datos similares que permitan acceder a la totalidad o a una parte del sistema.

En este apartado se incluyen cualquier tipo de contraseñas o códigos establecidos como medios para hacer posible el acceso a un sistema o a una parte del mismo. Se trata, por tanto, de medidas de seguridad para evitar la intromisión en archivos, partes de un sistema o en el sistema mismo, por quien no se encuentra habilitado para ello. En este apartado, a diferencia del anterior, el precepto no hace referencia a supuestas herramientas elaboradas específicamente para hacer posible la intromisión ilegítima en un sistema sino a la disponibilidad de las legítimamente creadas y utilizadas para el acceso regular al mismo.

En realidad, en estos casos, el Legislador, siguiendo los criterios de la Directiva, hace acreedoras de sanción penal situaciones claramente diferentes de las reseñadas en el apartado anterior. Se trata en definitiva de castigar la adquisición, en cualquier forma, para el propio uso o para facilitarla a terceros, de contraseñas o códigos de acceso ajenos con la finalidad de emplearlas en la ejecución de las actividades ilícitas a las que se refiere el artículo examinado. Es por ello que, en este caso, la conducta típica *producir*, difícilmente será aplicable, porque no se trata de fabricar algo nuevo sino de lograr la disponibilidad de algo ya existente. En cuanto a la adquisición para el propio uso ha de entenderse incluye tanto los supuestos de obtención a través de otra persona como aquellos en los que la disponibilidad de las claves se logra irregularmente por el propio poseedor. Lo importante a esos efectos es que dicha adquisición y/o posesión o facilitación a

terceros se lleve a efecto en las condiciones antes indicadas, es decir, sin autorización de la persona o personas legítimamente autorizadas para acceder al sistema y con la finalidad específica de cometer alguno de los delitos a que se refiere el precepto.

En el supuesto de que la misma persona que haya producido, importado o adquirido estas herramientas o instrumentos sea quien comete posteriormente el delito concreto, bien se trate de un delito contra la intimidad del art. 197 apartados 1 y 2 ó bien de alguno de los delitos previstos en el art. 197 bis, es decir acceso ilegal a sistemas informáticos o interceptación ilegal de transmisiones de datos entre sistemas, utilizando esos mismos medios fabricados, adquiridos o poseídos a dicho fin, ha de entenderse que se produce un concurso de normas, a resolver de acuerdo con el criterio de absorción previsto en el art. 8.3 del CP.

1.5 El nuevo art. 197 quater CP

Establece este precepto que *si los hechos descritos en este Capítulo se hubieran cometido en el seno de una organización o grupo criminal, se aplicarán respectivamente las penas superiores en grado.*

Además de la nueva ubicación sistemática el precepto refiere la aplicación de la agravante a todos los delitos recogidos en el Capítulo I del Título X, dedicado a los delitos de descubrimiento y revelación de secretos. La precisión es importante porque en la anterior redacción, vigente hasta el 1 de julio, la agravación incluida en el apartado 8 del art. 197 alcanzaba únicamente a los hechos descritos en los apartados precedentes de ese mismo precepto.

Esta modificación determina que la agravación sea susceptible de apreciarse, además de en todos los supuestos hasta ahora mencionados, en los previstos en el art. 199 CP, referidos a la revelación de secretos ajenos conocidos por razón del propio oficio o de las relaciones laborales y a la que lleva a efecto el profesional

incumpliendo sus obligaciones de sigilo o reserva, que en la regulación derogada, y por su ubicación sistemática, quedaban al margen de la aplicación de dicha circunstancia, sin perjuicio de que pudiera ser tenida en cuenta por la vía de los arts. 570 bis y ss del CP.

Como ya se indicó en la Circular 2/2011 de la Fiscalía General del Estado, *sobre la Reforma del Código Penal por Ley Orgánica 5/2010 en relación con las organizaciones y grupos criminales,* en estas ocasiones cuando el sujeto activo de estos delitos sea, al tiempo, integrante y/o dirigente del grupo u organización en cuyo seno se lleva a efecto la acción ilícita se produce un concurso de normas con los arts. 570 bis o 570 ter del CP. Es procedente por tanto recordar aquí el criterio establecido en dicha Circular que, en aplicación de lo establecido en art. 570 quáter in fine, remite en estos casos a la regla 4ª del art. 8º CP, y por tanto establece que *en tales supuestos los Sres. Fiscales cuidarán de aplicar, de acuerdo con lo dispuesto en el art 570 quater CP, conforme al criterio de alternatividad, un concurso de delitos entre el art. 570 bis o el art. 570 ter, en su caso y el tipo correspondiente al delito específicamente cometido con todas sus circunstancias si bien prescindiendo de la agravación específica de organización, cuando la pena así aplicada sea superior a la que prevé el subtipo agravado.*

Además del estudio que se contiene en dicha Circular son numerosas las Sentencias del Tribunal Supremo que, tras la entrada en vigor de los citados artículos, han ido perfilando la distinción entre los supuestos de organización y grupo criminal y los de simple codelincuencia. Pueden citarse entre otras, las SSTS nº 544/2012 de 2 de julio; 719/2013 de 9 de octubre; 576/2014 de 18 de julio y 603/2014 de 23 de septiembre.

Fiel exponente de esta doctrina es la STS nº 798/2016 de 25 de octubre que haciendo suya la doctrina fijada por la STS nº 644/2015 de 13 de octubre señala al respecto que *la organización y el grupo criminal tienen en común la unión o*

agrupación de dos o más personas y la finalidad de cometer delitos concertadamente. Pero mientras que la organización criminal requiere, además, la estabilidad o constitución por tiempo indefinido y que se repartan las tareas o funciones de manera concertada y coordinada (necesariamente ambos requisitos conjuntamente: estabilidad y reparto de tareas), el grupo criminal puede apreciarse cuando no concurra ninguno de estos dos requisitos o cuando concurra uno solo. De esta forma se reserva el concepto de organización criminal para aquellos supuestos de mayor complejidad en la estructura organizativa, pues es, precisamente, la estabilidad temporal y la complejidad estructural lo que justifica una mayor sanción en atención al importante incremento en la capacidad de lesión.

Por su parte la STS nº 787/2014, de 26 de noviembre, en orden a fijar la diferencia entre el grupo criminal y los supuestos de simple codelincuencia o coparticipación recuerda que *es conveniente tener en cuenta lo expresado en la Convención de Palermo al definir el grupo organizado: un grupo no formado fortuitamente para la comisión inmediata de un delito. Tanto la organización como el grupo están predeterminados a la comisión de una pluralidad de hechos delictivos. Por ello cuando se forme una agrupación de personas para la comisión de un delito específico, nos encontraremos ante un supuesto de codelincuencia, en el que no procede aplicar las figuras de grupo ni de organización*

En igual sentido la más reciente STS nº 128/2015, de 25 de febrero, recuerda que *la mera pluralidad de personas aun con una cierta -y obvia- planificación para la comisión de un ilícito penal, no constituye una organización criminal ni menos un grupo. La codelincuencia viene a ser un simple consorcio ocasional para la comisión de un delito en tanto que tanto la organización criminal como el grupo criminal constituye un aliud en relación a la codelincuencia, sin perjuicio de recordar, a su vez, las diferencias entre la organización y el grupo a las que ya se ha hecho referencia.*

1.6 El nuevo art. 197 quinquies CP.

La LO 1/2015 incorpora este nuevo precepto para establecer las penas correspondientes a las personas jurídicas cuando éstas resulten responsables de alguno de los delitos que se mencionan en el propio artículo, conforme a lo dispuesto en el art. 31 bis del CP.

Esta previsión ya estaba contemplada en el párrafo segundo del art. 197-3º CP, en su versión anterior a la reforma, tal y como quedó redactada por Ley Orgánica 5/2010 de 22 de Junio, y era de aplicación a todos los supuestos recogidos en el art. 197 CP.

La redacción del nuevo precepto es la siguiente:

Cuando de acuerdo con lo establecido en el art. 31 bis una persona jurídica sea responsable de los delitos comprendidos en los artículos 197, 197 bis y 197 ter, se le impondrá la pena de multa de seis meses a dos años. Atendidas las reglas establecidas en el art. 66 bis, los jueces y tribunales podrán asimismo imponer las penas recogidas en las letras b) a g) del apartado 7 del art. 33

Nótese que la reubicación sistemática del precepto, en coherencia con las modificaciones que se han introducido en el Capítulo y que se han venido comentando, ha ido acompañada de una variación en la indicación de los tipos penales a los que es aplicable de tal forma que la posibilidad de exigir responsabilidad a las personas jurídicas se hace extensiva a los nuevos delitos incorporados por la LO 1/2015.

1.7 El articulo 198 CP.

Este precepto no se ha visto afectado por la reforma operada por la LO 1/2015, y mantiene íntegramente su redacción en los siguientes términos:

La autoridad o funcionario público que, fuera de los casos permitidos por la Ley, sin mediar causa legal por delito, y prevaliéndose de su cargo, realizare cualquiera de las conductas descritas en el artículo anterior, será castigado con las penas respectivamente previstas en el mismo, en su mitad superior y, además, con la de inhabilitación absoluta por tiempo de seis a doce años.

Este precepto, en la regulación precedente, se encontraba situado a continuación del art. 197 CP, por lo que la mención del *artículo anterior* era una clara remisión a la totalidad de las conductas sancionadas en el mismo. Sin embargo, la nueva regulación que incorpora los artículos 197 bis, ter, quater y quinquies y la consiguiente reubicación sistemática del que se analiza, tras el art. 197 quinquies, hace que la referencia al *artículo anterior,* resulte incongruente ya que dicho precepto se refiere a las sanciones que, en su caso, procedería imponer a las personas jurídicas por este tipo de conductas.

En consecuencia, una interpretación sistemática de la norma lleva necesariamente a entender que dicha referencia lo es a todos los tipos penales de los que también pueden ser responsables las personas jurídicas, y que concretamente se mencionan en el art. 197 quinquies, es decir los hechos ilícitos tipificados en los artículos 197, 197 bis y 197 ter CP.

En relación con este tema, resulta conveniente traer a colación las diferencias entre el precepto que nos ocupa que sanciona al funcionario que fuera de los casos permitidos por la ley realiza cualquiera de las conductas indicadas y, entre ellas, la prevista en el artículo 197.3 consistente en *revelar o ceder a terceros los datos o hechos descubiertos o las imágenes captadas a que se refieren los números anteriores* y el artículo 417 que sanciona *a la autoridad o funcionario público que revelare secretos o informaciones de los que tenga conocimiento por razón de su oficio o cargo y que no deban ser divulgados.*

En el primer caso se trata de revelación o cesión a otros de información que se ha obtenido ilícitamente, en cualquiera de las formas previstas en el artículo 197.1 y 2, por el propio funcionario o autoridad o por un tercero, teniendo quien desvela el secreto conocimiento de la ilicitud de su obtención, en tanto que en el segundo supuesto, las informaciones o secretos que se revelan habrían llegado a conocimiento previo del funcionario o autoridad en el ejercicio de sus funciones y por razón de su oficio o cargo. Es decir, en este último supuesto, el acceso a la información se encuentra plenamente amparado por la ley, produciéndose la acción delictiva como consecuencia del incumplimiento por parte del propio funcionario o autoridad de sus deberes de sigilo.

En igual sentido se ha pronunciado la Sala Segunda del Tribunal Supremo en sus sentencias, entre otras nº 377/2013 de 3 de mayo y 525/2014 de 17 de junio, a cuyo tenor *la diferencia esencial entre las conductas contempladas en los artículos 197 y 198 y el artículo 417 del C. P cometidos por un funcionario o autoridad, se centra en la legalidad del acceso a la información reservada a la que se refieren dichos preceptos. El artículo 197 parte de la exigencia de que el autor no esté autorizado para el acceso, el apoderamiento, la utilización o la modificación en relación a los datos reservados de carácter personal o familiar y castiga en el artículo 198 a la autoridad o funcionario público, que fuera de los casos permitidos por la ley, sin mediar causa legal por delito y prevaliéndose de su cargo, realizare cualquiera de las conductas descritas en el artículo anterior. Mientras que el artículo 417 castiga la revelación de secretos o informaciones que no deben ser divulgados y de los que la autoridad o funcionario público haya tenido conocimiento por razón de su oficio o cargo.*

1.8 Condiciones de perseguibilidad de estas conductas

La incorporación de los nuevos preceptos examinados, artículo 197 bis y ter, al Capítulo I del Título X del Libro II del CP hace que la previsión establecida en el art. 201 del Código penal -a cuyo tenor *para proceder por los delitos previstos en este*

capítulo será necesaria denuncia de la persona agraviada o de su representante legal, sin perjuicio de las facultades asignadas al Ministerio Fiscal cuando el agraviado fuera una persona menor de edad o en situación de discapacidad -extienda sus efectos sobre los mismos. Indica igualmente dicho precepto que esta denuncia no será exigible *cuando la comisión del delito afecte a los intereses generales o a una pluralidad de personas* o cuando el delito fuera cometido por autoridad o funcionario público prevaliéndose de su cargo (art 198 CP). A su vez el apartado 3º del precepto examinado atribuye al perdón del ofendido o de su representante legal la capacidad de extinguir la acción penal.

La exigencia de denuncia previa del agraviado es plenamente coherente con las necesidades de protección penal frente a conductas que atentan contra bienes de carácter estrictamente personal, como el derecho a la intimidad, pero no lo es tanto en referencia a estos nuevos tipos penales en los que lo que se sanciona es, en palabras del Preámbulo de la norma, *el acceso a otros datos o informaciones que pueden afectar a la privacidad pero que no están referidos directamente a la intimidad personal*, pues, como claramente se explica, no es lo mismo la pretensión de apoderarse o tomar conocimiento del listado de contactos de una persona que realizar la acción ilícita con el objeto de averiguar las características de un determinado programa informático.

En cualquier caso, esta exigencia de denuncia de la persona agraviada o de su representante legal, como requisito de procedibilidad, tiene como consecuencia respecto de los supuestos -conocidos como *hacking ético* o *hacking blanco*- en que la intrusión ilegal se lleva a efecto con la finalidad de descubrir las vulnerabilidades del sistema para informar de ello al titular del mismo, que la posibilidad de actuar penalmente frente a estas conductas quede a expensas de la efectiva presentación de denuncia - o de la ausencia de perdón- por parte de quien se ha visto afectado por ese comportamiento que, en ocasiones, puede reportarle un beneficio al permitirle conocer y subsanar los fallos de seguridad del propio sistema

Al margen de ello, ha de indicarse que el planteamiento de la Directiva 2013/40/UE, que se incorpora a nuestro ordenamiento jurídico a través de estos preceptos, se articula en torno a la necesidad de proteger no tanto intereses de carácter particular como aquellos de carácter más general o colectivo que pueden verse afectados seriamente por la utilización de los avances tecnológicos en la comisión de actividades ilícitas, particularmente cuando las nuevas herramientas e instrumentos sirvan como medio para la planificación y ejecución de ataques a los sistemas informáticos con el objetivo de obtener información de organismos e instituciones de carácter público o encargados de gestionar intereses esenciales para los ciudadanos.

Por ello, la exigencia de denuncia del agraviado para proceder por estos delitos puede resultar perturbadora en la aplicación de algunos de los nuevos preceptos, especialmente en lo que se refiere al art. 197 ter CP, dado que en los supuestos que en él se sancionan -actos preparatorios del ataque informático en sí mismo- no resulta necesario, para integrar todos los elementos del tipo penal, que la acción se haya concretado en datos o sistemas informáticos específicos, y por tanto que la conducta ejecutada haya llegado a *agraviar* -al menos directamente- a persona o personas determinadas.

Esta circunstancia, no obstante, se solventa, en buena medida, con la previsión recogida en el apartado segundo del citado art. 201 CP que hace innecesaria dicha denuncia previa en los supuestos en que la comisión del delito afecte a intereses generales o a una pluralidad de personas, circunstancia que habrá de valorarse en atención al número o características del sistema o sistemas informáticos objeto de acceso o interceptación ilegal o, en los supuestos del art. 197 ter, cuando, en el curso de la investigación, se haya podido concretar -en mayor o menor medida- el fin a que se destinaban las herramientas o instrumentos o, dicho de otro modo, los sistemas o dispositivos en relación con los cuales se preparaba el ataque o el acto de espionaje informático.

En cuanto a lo que haya de entenderse por *pluralidad de personas* la reciente STS 201/2017 de 21 de marzo precisa que *pluralidad indica algo más que varios unos,* añadiendo que la utilización de dicho término *sería sinónimo de multiplicidad*. Desde este planteamiento no sería necesaria la denuncia previa cuando el objeto de la acción ilícita fuera el espionaje informático de organismos e instituciones del Estado, o cuando lo que se pretenda sea la obtención masiva de credenciales bancarias de una pluralidad de ciudadanos o acciones de similar naturaleza planificadas para afectar a muchas personas.

2. Novedades introducidas en los delitos de daños informáticos

Las variaciones incorporadas por la LO 1/2015 en los delitos de daños informáticos son el resultado de la implementación en nuestro ordenamiento jurídico penal de la Directiva 2013/40/UE del Parlamento y del Consejo, de 12 de agosto, relativa a los ataques contra los sistemas de información. A su vez, esta Directiva, hace suyos los planteamientos de la Convención de Budapest. En los estudios previos a la elaboración de dicha Convención se dejó constancia de que lo que se pretende a través de estos preceptos legales es otorgar a los datos y programas informáticos una protección similar a la que tienen los objetos corpóreos frente a daños causados de forma deliberada.

Ha de recordarse que el art. 264 CP, en su redacción previa a esta reforma, había sido introducido en el CP por Ley Orgánica 5/2010, de 22 de junio, para dar cumplimiento a la Decisión Marco 2005/222/JAI del Consejo, de 24 de junio. La sustitución de dicha Decisión Marco por la Directiva del año 2013 ha determinado la necesidad de acomodar nuestra legislación criminal a los parámetros fijados por esta última con la finalidad de ofrecer respuestas a los problemas y situaciones derivados de las novedosas manifestaciones de ataques masivos y coordinados a sistemas de información.

Destaca en primer término la reorganización sistemática de los artículos en los que se definen y sancionan este tipo de conductas. Efectivamente, el Legislador, apartándose del criterio seguido en la anterior regulación, ha estimado oportuno tipificar y sancionar en artículos separados las conductas ilícitas dirigidas contra datos informáticos, programas informáticos y documentos electrónicos ajenos, de aquellas otras cuyo objeto es el de obstaculizar o interrumpir el normal funcionamiento de sistemas informáticos; recogiendo las primeras en el art. 264, que recibe nueva redacción, e incorporando un nuevo precepto, el 264 bis, para los delitos relativos a los daños sobre sistemas informáticos. Con ello se realiza una adaptación de nuestra normativa interna más fiel a la Directiva europea, que contempla separadamente los dos tipos de conductas: las primeras en el art. 5 subtitulado como *Interferencia ilegal en los datos* y las segundas en el art. 4 bajo el epígrafe *Interferencia ilegal en los sistemas de información.*

2.1 Nueva redacción del art. 264 CP.

De acuerdo con este criterio el art. 264 CP queda redactado en la siguiente forma:

1. El que por cualquier medio, sin autorización y de manera grave borrase, dañase, deteriorase, alterase, suprimiese o hiciese inaccesibles datos informáticos, programas informáticos o documentos electrónicos ajenos, cuando el resultado producido fuera grave, será castigado con la pena de prisión de seis meses a tres años.
2. Se impondrá una pena de prisión de dos a cinco años y multa del tanto al décuplo del perjuicio ocasionado, cuando en las conductas descritas concurra alguna de las siguientes circunstancias:

1ª Se hubiese cometido en el marco de una organización criminal.
2ª Haya ocasionado daños de especial gravedad o afectado a un número elevado de sistemas informáticos.

3ª El hecho hubiera perjudicado gravemente el funcionamiento de servicios públicos esenciales o la provisión de bienes de primera necesidad.
4ª Los hechos hayan afectado al sistema informático de una infraestructura crítica o se hubiera creado una situación de peligro grave para la seguridad del Estado, de la Unión Europea o de un Estado Miembro de la Unión Europea. A estos efectos se considerará infraestructura crítica un elemento, sistema o parte de este que sea esencial para el mantenimiento de funciones vitales de la sociedad, la salud, la seguridad, la protección y el bienestar económico y social de la población cuya perturbación o destrucción tendría un impacto significativo al no poder mantener sus funciones.
5ª El delito se haya cometido utilizando alguno de los medios a que se refiere el art. 264 ter.

Si los hechos hubieran resultado de extrema gravedad, podrá imponerse la pena superior en grado.

3. Las penas previstas en los apartados anteriores se impondrán, en sus respectivos casos, en su mitad superior, cuando los hechos se hubieran cometido mediante la utilización ilícita de datos personales de otra persona para facilitarse el acceso al sistema informático o para ganarse la confianza de un tercero.

Se mantienen como conductas típicas las de borrar, dañar, deteriorar, alterar, suprimir y hacer inaccesibles, ya contempladas en la legislación precedente, siguiendo también en este aspecto la relación de comportamientos que recogen la Directiva 2013/40/UE en su art. 5, relativo a la interferencia ilegal en los datos, y la Decisión Marco 2005/22/JAI en su art. 4. De esta forma el Legislador pretende abarcar todas las posibles conductas susceptibles de afectar a los elementos informáticos, tanto aquellas que impliquen su destrucción, bien sea total o parcial, como aquellas otras que comporten una modificación *-alteración-* de los mismos que igual podría producirse por eliminación, supresión o borrado parcial del

elemento afectado como por la incorporación de nuevos datos que impliquen la variación del alcance o contenido inicial de aquellos.

La conducta de *hacer inaccesible* abarca aquellos supuestos en los que la acción ilícita, ejercida sobre los datos y/o programas informáticos o documentos electrónicos, produce como consecuencia, sin afectar a la existencia o esencia de los mismos, la imposibilidad de acceder a ellos ya sea para conocer su contenido, para operar con ellos o, en general, para utilizarlos en cualquier modo. Un buen ejemplo de este efecto es el que produce el programa malicioso conocido como *ransomware*, que restringe el acceso a determinadas partes o archivos del sistema infectado, generalmente a través de su cifrado, situación que, en principio, solo podría solventarse, y así lo suele plantear el atacante informático, abonando el rescate que con esa finalidad reclama a sus víctimas.

La reforma operada en este precepto por LO 1/2015, además de limitar su aplicación a los ataques contra datos, programas informáticos y documentos electrónicos ajenos, ofrece novedades destacables en las sanciones imponibles por dichos ilícitos y también en la definición de los subtipos agravados

2.1.1 Los subtipos agravados del art. 264.2 C. Penal.

La LO 1/2015 mantiene la primera de las agravaciones que ya contemplaba el art. 264.3º CP, en su redacción anterior al 1 de julio de 2015, en iguales términos aunque con modificaciones penológicas, y sustituye la segunda de las agravaciones previstas en el mismo apartado, referida a los supuestos en que se hubieran ocasionado daños de especial gravedad o afectado a los intereses generales, por las recogidas en los números 2º a 5º del apartado segundo del nuevo precepto.

Pese a su ubicación, estos subtipos agravados son aplicables tanto a los delitos de daños en datos, programas informáticos o documentos electrónicos ajenos como a

las conductas de interrupción u obstaculización de sistemas informáticos, por mor de la remisión que el apartado segundo del art. 264 bis hace al precepto analizado.

Por tanto, tras la reforma, la configuración de los subtipos agravados es la siguiente:

1º Se hubiera cometido en el marco de una organización criminal

Se trata de una circunstancia de agravación plenamente conforme con el criterio que fija al respecto la Directiva europea en su decimotercer considerando, al recordar a los Estados la conveniencia de establecer sanciones más severas cuando el ataque se cometa en el contexto de una organización delictiva tal y como se define en la Decisión Marco 2008/841/JAI del Consejo, de 24 de octubre, relativa a la lucha contra la delincuencia organizada.

En relación con esta circunstancia habrán de tenerse en cuenta los criterios establecidos en la Circular 2/2011 anteriormente comentados, en los casos en que concurran en una misma persona el carácter de sujeto activo de este delito y de alguno de los hechos ilícitos contemplados en el art. 570 bis del CP.

Nótese, no obstante, que la referencia lo es, exclusivamente, a organización criminal, no a grupo criminal, por lo que en este último supuesto habría de aplicarse un concurso real de delitos, entre el que nos ocupa y sus circunstancias y el del art. 570 ter, cuando el sujeto activo del delito de daños constituya, financie o integre a su vez un grupo criminal, en las circunstancias y condiciones que se establecen en dicho precepto.

2º *Haya ocasionado daños de especial gravedad o afectado a un número elevado de sistemas informáticos.*

El primer inciso de este subtipo estaba ya contemplado en la anterior redacción, añadiéndose en el nuevo texto la inclusión de los supuestos en que hayan resultado afectados un número elevado de sistemas informáticos. Ambas circunstancias se encuentran enlazadas por la conjunción disyuntiva “o”, lo que ha de interpretarse en el sentido de que no han de concurrir conjuntamente sino que la agravación puede aplicarse aun cuando solo sea apreciable una u otra de ellas. Puede tratarse por tanto de daños de especial gravedad causados en uno solo o en una pluralidad de sistemas de información o de una acción que genere efectos en un número importante de sistemas, aun cuando el daño causado en cada uno de ellos no sea de especial gravedad, si el volumen de sistemas afectados justifica la aplicación de la agravación.

En relación con ambas circunstancias ha de reseñarse en primer lugar la imprecisión de los términos empleados por el Legislador, lo que obligará a una labor exegética que habrá de ser completada por los criterios jurisprudenciales que se vayan elaborando al respecto.

Particularmente llama la atención que en el precepto examinado el parámetro *gravedad,* en referencia a la acción, al resultado, al daño causado o a los hechos en su conjunto, se utilice con tres finalidades distintas: en el apartado primero al definir los requisitos del tipo, ya que la acción solo será delictiva si la conducta se realiza de *manera grave* y *si el resultado producido fuera grave;* en el apartado segundo, circunstancia segunda, para delimitar la aplicación de agravante a los supuestos en que se hayan ocasionado daños de *especial gravedad* , y en el inciso último de este mismo apartado para hacer posible la imposición de la pena superior en grado cuando *los hechos hubieran resultado de extrema gravedad*. Es decir la gravedad de la acción y de su resultado no solamente es determinante de la tipicidad de la conducta sino también de la aplicación de un subtipo agravado y de un posterior incremento punitivo en grado, en los casos más extremos. Sin embargo, y pese a su trascendencia a estos efectos, la determinación de criterios en orden a una adecuada valoración de dicho calificativo presenta cierta dificultad.

Al respecto, se hace necesario destacar que tanto en el tipo básico como en el párrafo último del apartado 2º, que como cláusula de cierre contempla los efectos penológicos en los supuestos de extrema gravedad, el uso de este calificativo se refiere al delito en su conjunto. Así en el tipo básico se concreta tanto en el modo de ejecución - *manera grave*- como en el resultado de la acción y en los casos de extrema gravedad en una referencia genérica a los hechos resultantes. Sin embargo en el subtipo que se examina dicho criterio valorativo se pone en relación con los daños ocasionados, es decir, en los efectos, materiales e inmateriales, derivados de la acción ilícita, si bien, no ha de olvidarse, que para que la conducta sea típica es imprescindible que la misma se lleve a efecto de manera grave y que además el resultado sea grave. Quiere decirse con ello que procedería la aplicación de esta agravante cuando, concurriendo los requisitos del tipo básico, los efectos lesivos causados por el delito merecieran por su entidad la consideración de especialmente graves y además no estuvieran incluidos en ninguno de los supuestos previstos en los restantes subtipos contemplados en el mismo artículo.

En el análisis de esta cuestión no puede prescindirse del alcance y sentido de la acción típica. Es decir, en ningún caso puede obviarse que lo que se sanciona en este precepto son las conductas de borrar, dañar, deteriorar, alterar, suprimir o hacer inaccesibles datos o programas informáticos y/o documentos electrónicos ajenos y que dichas conductas no tienen por qué estar vinculadas a actos materiales que impliquen alteración, destrucción o inutilización de soportes físicos, es más, en la mayoría de los supuestos no se verán afectados por la actividad ilícita dichos elementos o soportes físicos. Ha de tenerse en cuenta que el objeto de la acción típica no son las herramientas, dispositivos o elementos externos (*hardware*), a través de las cuales operamos informáticamente, sino los elementos lógicos o de carácter inmaterial (*software*) de un sistema de información. En relación con ello es importante recordar que tanto la Decisión Marco 2005/222/JAI del Consejo, de 24 de febrero, de cuya implementación deriva el art. 264 CP en su

inicial redacción, como la Directiva 2013/40/UE, incorporada por la Ley Orgánica 1/2015, tienen por objeto el establecimiento de criterios comunes para sancionar penalmente los ataques contra los sistemas de información que se llevan a efecto en el ciberespacio a través, por tanto, de las tecnologías de la información y la comunicación y en el ámbito de realidades de carácter virtual.

A los efectos de definir el objeto de la acción ilícita, debe recordarse que la citada Directiva 2013/40/UE en su art. 2º b) considera como *datos informáticos*, *toda representación de hechos, informaciones o conceptos de una forma que permite su tratamiento por un sistema de información, incluidos los programas* (informáticos) a los que, a su vez, se refiere como *aquellos que sirven para hacer que dicho sistema de información realice una función.*

Por su parte el documento electrónico ha sido definido por el art 3.5 de la Ley 59/2003 de 19 de diciembre, *sobre firma electrónica* 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*. La Norma Técnica de Interoperabilidad del Documento Electrónico, aprobada por resolución de 19 de julio de 2011 de la Secretaría de Estado para la Función Pública, establece los componentes de estos documentos incluyendo contenido, firma electrónica y metadatos mínimos obligatorios así como su formato y las condiciones para su intercambio y reproducción.

Por tanto, los resultados derivados de este tipo de acciones no tienen por qué afectar a la integridad física de uno o varios objetos sino que, en muchas ocasiones, sus consecuencias serán de carácter exclusivamente inmaterial concretándose en definitiva, y en palabras de la Convención de Budapest, en la disponibilidad y/o integridad de la información que, en su caso, se haya visto dañada alterada, suprimida o haya resultado inaccesible, o en la propia funcionalidad u operatividad del programa o programas que se hayan visto afectados como consecuencia de la actividad ilícita.

Es decir, el delito de daños informáticos no requiere un ataque a la integridad física del objeto sino que la acción sobre los elementos lógicos puede ejecutarse a través de procedimientos informáticos. Por eso mismo para valorar la gravedad de la conducta y/o de su resultado no puede trasladarse a los delitos informáticos la cuantía diferenciadora de los 400 euros, prevista en el art. 263 CP a efectos punitivos para los daños clásicos, pues esta cuantía se refiere al menoscabo que sufre un objeto material, mientras que los delitos informáticos tienen por objeto, como se ha dicho, elementos inmateriales.

Todo ello ha de considerarse en la valoración de los daños causados en orden a la aplicación de esta circunstancia de agravación. En consecuencia, los criterios que pueden ser apreciados, con el fin de cuantificar ese daño funcional, van desde el valor de la destrucción definitiva de los datos informáticos -con la dificultad que entraña esta valoración- al valor económico cuantificable del coste de restablecimiento de la operatividad de los datos, programas o, en su caso, del sistema afectado. Derivado de este último criterio está el del perjuicio económico que haya supuesto para la víctima o el afectado el periodo de tiempo en que los sistemas han permanecido inutilizados y/o el necesario para restaurar su funcionamiento, factores que estarán íntimamente ligados a la pérdida de capacidad de actuación o al lucro cesante sufrido por la imposibilidad de uso de los datos o sistemas durante ese lapso temporal, daños que serán más evidentes y graves para las entidades que tienen por objeto una actividad económica. No han de olvidarse tampoco, como criterio para la valoración del resultado de la acción típica, las consecuencias que podrían derivarse, a efectos de la reputación de una determinada empresa, entidad o persona física, del hecho de haber sido objeto de un ataque informático pues ello puede conllevar un perjuicio intangible por el daño causado a la imagen pública de aquéllas. Ha de recordarse al respecto que en ocasiones el atacante no tiene como objetivo ocasionar un daño patrimonial, sino producir un daño a la imagen de una determinado organismo o entidad provocando una pérdida de credibilidad o una desconfianza social hacia el mismo.

Finalmente habrán de tenerse en cuenta los perjuicios ocasionados no solamente para el directamente ofendido sino también para el interés general, los bienes jurídicos afectados por la acción ilícita, o el riesgo que se genera para intereses públicos o privados por causa de la perdida de los datos, programas o documentos etc.. En definitiva, todas estas consecuencias deberán analizarse caso a caso y en atención a las circunstancias concurrentes, lo que en muchos supuestos determinará la necesidad de recabar dictámenes técnicos y/o informes periciales en relación con los extremos antes indicados.

En orden a definir el límite a partir del cual un resultado puede considerarse grave o especialmente grave, a los efectos de la aplicación de esta circunstancia, es interesante reseñar, con carácter ilustrativo, que la Directiva europea al referirse en su quinto considerando a los ataques masivos, realizados a gran escala y susceptibles de causar graves daños, deriva a los Estados la competencia para delimitar dicho concepto de acuerdo con los criterios de los respectivos ordenamientos y prácticas nacionales, si bien ofrece algunas pautas para su valoración tales como *interrumpir los servicios del sistema de una importancia pública relevante o causar importantes costes económicos o pérdidas de datos de carácter personal o de información sensible*. A su vez, al referirse en su decimoprimer considerando a aquellos otros supuestos que pueden considerarse como de *menor gravedad*, y que en consecuencia pudieran quedar excluidos de sanción, facilita también algunos otros parámetros de valoración como la insignificancia del daño causado o del riesgo generado para intereses públicos o privados o para los derechos o intereses de las personas que resulten afectadas o , en su caso, el escaso nivel de afección en la integridad de los datos o de los sistemas.

En consecuencia y, a partir del indicado planteamiento, habrían de considerarse graves y, por tanto, encuadrables por su resultado en el art. 264.1º CP. todas aquellas acciones ilícitas, sobre los elementos lógicos, que tuvieran trascendencia

significativa o generaran consecuencias apreciables en datos, programas informáticos o documentos electrónicos o en los intereses en juego. Por su parte, procedería la aplicación del subtipo que nos ocupa en los supuestos en que los efectos del delito fueran especialmente relevantes y no se hicieran merecedores por su intensidad de la calificación de extrema gravedad a que se refiere el inciso último del mismo precepto. A los efectos de aplicar uno u otro precepto y como criterios de valoración habrían de tenerse en cuenta los anteriormente indicados y, en particular, como señala la SAP de Madrid 480/2017 de 10 de enero, *la posibilidad o no de recuperar los datos informáticos, la pérdida definitiva de los mismos o la posibilidad de recuperación y, en este último caso, el coste económico de la reparación del daño causado, la complejidad técnica de los trabajos de recuperación, la duración de las tareas de recuperación, el valor del perjuicio causado al titular de los datos, bien como lucro cesante o como daño emergente*.

En relación con el segundo inciso de este mismo apartado, que hace depender la agravación del elevado número de sistemas afectados, ha de reseñarse que la Directiva 2013/40/UE se refiere específicamente al sentido último de esta circunstancia al indicar en su considerando decimotercero que *es conveniente establecer sanciones más severas cuando el ciberataque se realiza a gran escala y afecta a un número importante de sistemas de información, en particular, cuando el ataque tiene por objeto crear una red infectada o si el ciberataque causa un daño grave, incluido cuando se lleva a cabo a través de una red infectada*. Es decir, que la razón de ser de la agravación, que se deriva directamente de dicha norma europea, está en el especial riesgo que generan aquellos ataques en los que se ven afectados un número considerable de ordenadores que a su vez, y tras ser infectados, pueden servir para poder llevar a efecto un posterior ataque masivo y coordinado.

Por ello, y con independencia de que la cantidad de sistemas informáticos afectados pueda ser un factor a tener en cuenta a efectos de integrar el primer inciso de este mismo apartado del art. 264.2 por ocasionar daños de especial

gravedad, la circunstancia recogida en el segundo inciso habría de aplicarse más específicamente en los supuestos en los que se vieran afectados un número tal de sistemas de información que pudieran generar el riesgo de un ataque masivo de dichas características.

3ª El hecho hubiera perjudicado gravemente el funcionamiento de servicios públicos esenciales o la provisión de bienes de primera necesidad.

La STC nº 26/1981, de 17 de julio, refiere el concepto de servicio esencial del art. 128.2 de la Constitución Española a aquellas actividades industriales o mercantiles de las que derivan prestaciones vitales o necesarias para la vida de una comunidad. Esta doctrina se completa con la establecida en STC nº 8/1992, de 16 de enero según la cual *antes que a determinadas actividades industriales y mercantiles, de las que se derivarían prestaciones vitales y necesarias para la vida de la comunidad, la noción de servicio esencial de la comunidad hace referencia a la naturaleza de los intereses a cuya satisfacción la prestación se endereza, entendiendo por tales los derechos fundamentales, las libertades públicas y los bienes constitucionalmente protegidos con la consecuencia de que a priori ningún tipo de actividad productiva puede ser considerado en sí mismo como esencial (STC 51/1986) solo lo será en aquellos casos en que la satisfacción de los mencionados exija el mantenimiento del servicio y en la medida y con la intensidad que efectivamente lo exija.* Por su parte, la Ley 8/2011, de 28 de abril, *por la que se establecen medidas para la protección de infraestructuras críticas*, define, en su art. 2, los servicios esenciales como *aquellos necesarios para el mantenimiento de las funciones sociales básicas, la salud, la seguridad, el bienestar social y económico de los ciudadanos, o el eficaz funcionamiento de las Instituciones del Estado y las Administraciones Públicas.*

Según el art. 128.2 CE los servicios esenciales podrán reservarse por ley al sector público y también podrá acordarse la intervención de empresas en la prestación de los mismos, cuando así lo exija el interés general. Se trata, por tanto, de servicios

indispensables para el funcionamiento de la sociedad que en ocasiones pueden prestarse por el sector público o también encomendarse a la iniciativa privada sometidos a una adecuada reglamentación, como es el caso de las telecomunicaciones, el transporte aéreo o la energía.

En cuanto a la referencia a bienes de primera necesidad, es claro que el Legislador alude a aquellos que son fundamentales para el desarrollo de la vida de los ciudadanos y para la atención de sus necesidades primarias. En relación con ello la STS nº 432/2003 de 26 de marzo, a propósito de un supuesto de estafa, recuerda que la Sala viene entendiendo que son bienes de primera necesidad *los alimentos, medicamentos, viviendas y otros productos de consumo necesario para la subsistencia y salud de las personas.* También son de interés a estos efectos la STS nº 232/2012, de 5 de marzo, a cuyo tenor *la categoría de "cosas de primera necesidad" se encuentra referida a aquellas "de las que no se puede prescindir", según el diccionario de la Real Academia, lo que esta Sala viene vinculando a productos de consumo imprescindible para la subsistencia o la salud de las personas,* y también la STS nº 1307/2006, de 22 de diciembre, que recuerda como doctrina del Tribunal, a efectos de la aplicación del delito de estafa del art. 250.1 CP, *que por cosas de primera necesidad o bienes de utilidad social, además de las viviendas expresamente mencionadas, habrá que entender todas aquellas que resulten imprescindibles para la subsistencia y salud de las personas.*

Por tanto, la agravación será aplicable cuando el ataque informático a datos, programas o documentos afecte gravemente a la prestación ordinaria de los indicados servicios esenciales o a la provisión de bienes de primera necesidad. También en este subtipo la utilización del adverbio *gravemente* supone la introducción de un criterio de valoración indeterminado, cuya concurrencia habrá de analizarse individualizadamente y en función del servicio o prestación de que se trate, pero que excluye en todo caso la aplicación de esta circunstancia cuando los efectos de la acción ilícita hayan resultado intrascendentes o no se hubiera generado una alteración apreciable en el funcionamiento de dichos servicios.

4ª Los hechos hayan afectado al sistema informático de una infraestructura crítica o se hubiera creado una situación de peligro grave para la seguridad del Estado, de la Unión Europea o de un Estado Miembro de la Unión Europea. A estos efectos se considerará infraestructura crítica un elemento, sistema o parte de este que sea esencial para el mantenimiento de funciones vitales de la sociedad, la salud, la seguridad, la protección y el bienestar económico y social de la población cuya perturbación o destrucción tendría un impacto significativo al no poder mantener sus funciones.

En relación con esta circunstancia es el propio Legislador el que define lo que ha de entenderse por infraestructura crítica. A estos efectos ha de tenerse en cuenta que la Ley 8/2011 prevé la existencia de un Catálogo Nacional de Infraestructuras Estratégicas, que es un registro de carácter administrativo en el que se recoge la información completa y actualizada de todas las infraestructuras estratégicas ubicadas en el territorio nacional, entre las que se hallan incluidas aquellas clasificadas como críticas o críticas europeas que afecten a España. No obstante, la concurrencia de dicha cualidad en el organismo u entidad cuyo sistema es atacado, en principio, podría no ser conocida por el autor del hecho, dado que el contenido del referido Catálogo tiene la consideración oficial de secreto, de conformidad con lo dispuesto en el art. 4.3 del RD 704/2011, de 20 de mayo, que aprueba el Reglamento de Protección de Infraestructuras Críticas. Por ello, y sin perjuicio de la posibilidad de obtener a posteriori una certificación oficial sobre dicho extremo, a los efectos de acreditar dicha condición en referencia al organismo e institución específicamente atacado, el hecho de que el Legislador haya optado por definir en el propio art. 264.2. 4º lo que ha de entenderse por infraestructura crítica facilita la interpretación del precepto sin necesidad de acudir a otras fuentes

La Directiva 2013/40/UE se refiere también a esta circunstancia agravatoria en los siguientes términos: *existen en la Unión una serie de infraestructuras críticas cuya*

perturbación o destrucción tendría repercusiones transfronterizas importantes. De la necesidad de incrementar en la Unión la capacidad de protección de estas infraestructuras se desprende que las medidas contra los ataques informáticos deben complementarse con penas estrictas que reflejen la gravedad de tales ataques. A estos efectos la Directiva utiliza una definición muy similar a la que recoge el precepto que nos ocupa y que ilustra citando, a modo de ejemplo, *las centrales eléctricas, las redes de transporte y las redes de los órganos de gobierno.*

La agravación operará con la simple afección al sistema informático de una infraestructura de esta naturaleza, siempre que concurran los requisitos del tipo básico, sin precisar para su apreciación que la incidencia en datos o programas o en el propio sistema haya afectado, en forma grave, al funcionamiento o normal actividad de la entidad u organismo atacado. Por el contrario, y en relación con el segundo inciso referido a la creación de un peligro para la seguridad del Estado, de la Unión Europea o de un Estado Miembro de la Unión Europea, el Legislador exige para la estimación de esta circunstancia que el peligro sea efectivamente grave.

A propósito de la interpretación de este precepto no ha de olvidarse que, según establece el art. 573.2 CP, se considerarán delitos de terrorismo los delitos informáticos tipificados en los artículos 197 bis y 197 ter y 264 a 264 quater cuando los hechos se cometan con alguna de las finalidades recogidas en el art. 573.1 del mismo texto legal. Este último precepto, en su redacción derivada de la reforma operada por LO 2/2015, considera que concurre la citada finalidad cuando, a través de cualquiera de las conductas indicadas, lo que se pretende es alguno de los siguientes objetivos:

1ª Subvertir el orden constitucional, o suprimir o desestabilizar gravemente el funcionamiento de las instituciones políticas o de las estructuras económicas o sociales del Estado, u obligar a los poderes públicos a realizar un acto o a abstenerse de hacerlo.

2ª Alterar gravemente la paz pública.

3ª Desestabilizar gravemente el funcionamiento de una organización internacional.

4ª Provocar un estado de terror en la población o en una parte de ella.

Por tanto, cualquiera de los delitos que menciona el art. 573.2 CP, integraría un delito de terrorismo si se lleva a efecto con una de las finalidades indicadas. Ahora bien, va a ser precisamente en los supuestos en que concurran alguna o algunas de las agravaciones que se están examinando cuando dicha posibilidad resultará más evidente, ya que si un ataque informático perjudica gravemente la prestación de servicios esenciales, afecta a infraestructuras críticas o implica un grave peligro para la seguridad de los Estados o de la Unión Europea, es muy probable que la finalidad que se pretende con el ataque informático pueda considerarse de carácter terrorista. En estos casos se generará un concurso de normas a resolver por el principio de especialidad de conformidad con lo establecido en el art. 8.1º del CP y en el propio art. 573.2 CP, solución legal con efectos no solamente en orden a la calificación jurídica y sanción de la conducta sino también de competencia objetiva, ya que la instrucción y enjuiciamiento de esas tipologías delictivas viene asignada en exclusividad a los órganos de la Audiencia Nacional, en aplicación de lo establecido en la Disposición Transitoria de la Ley Orgánica 4/1988, de 25 de mayo, de reforma de la Ley de Enjuiciamiento Criminal.

5ª El delito se haya cometido utilizando alguno de los medios a que se refiere el art. 264 ter.

El precepto sanciona más gravemente la comisión del acto ilícito cuando en la acción se utilizan algunas de las herramientas a que se refiere el nuevo art. 264 ter, es decir: programas informáticos concebidos o adaptados principalmente para cometer estos delitos o contraseñas de ordenador, códigos de acceso o datos similares que permitan acceder a la totalidad o a una parte de un sistema de

información. Ya se ha indicado anteriormente, al comentar el art. 197 ter, de similar redacción, cual ha de ser la interpretación de estos conceptos y también cuales son las razones por las que el Legislador europeo ha estimado conveniente adelantar la barrera de protección y sancionar penalmente determinadas conductas relacionadas con la elaboración, adquisición o transmisión a terceros de estas herramientas o instrumentos informáticos.

La Directiva, que se refiere a la concurrencia de esta circunstancia en su art. 9º y en sus considerandos 13º y 16º, reflexiona acerca de la especial gravedad de la utilización de programas maliciosos (*malware*) diseñados y/o adaptados para cometer estas conductas de forma masiva e indiscriminada. Al respecto ha de indicarse que cuando este sea el supuesto que determina la aplicación de la agravación, y ello dé lugar a la infección de un número elevado de sistemas, dicha circunstancia pudiera concurrir con la prevista en el inciso segundo del art. 264.2.2º CP, como anteriormente ya se ha señalado.

Ahora bien, distinto será el supuesto en el que las herramientas utilizadas sean programas informáticos maliciosos concebidos para efectuar ataques informáticos de carácter aislado o individualizado o, cuando lo que se usa sean contraseñas de ordenador, códigos de acceso o datos similares que hagan factible la intromisión en un sistema de información perfectamente determinado. El empleo de estas herramientas o de las claves y códigos, en principio diferentes en cada uno de los sistemas, no tiene por qué estar vinculado a ataques informáticos plurales. Ello es especialmente claro en lo que respecta al uso de contraseñas o claves de acceso ajenas, que es el mecanismo que se utilizará con frecuencia en muchas de las acciones ilícitas cuyo objeto sean datos, programas o sistemas informáticos aisladamente considerados. Por esta razón llama la atención que el Legislador haya optado por penalizar la utilización de estas claves, perfectamente individualizadas, con una sanción considerablemente más elevada que la correspondiente al tipo básico, en el cual, por definición legal, la acción de borrar, dañar, deteriorar, alterar, suprimir o hacer inaccesibles los efectos inmateriales

protegidos puede llevarse a efecto por cualquier medio. En atención a ello, los Sres. Fiscales deberán valorar con especial cautela la aplicación de este subtipo en estos últimos supuestos restringiendo su apreciación a aquellos casos en los que el uso de dichas claves o contraseñas implique efectivamente un incremento en el plus de antijuridicidad de la conducta.

2.1.2 La agravación especifica del art. 264.3 CP.

Finalmente el apartado tercero del art. 264 CP establece, de forma preceptiva, la imposición de las penas en su mitad superior, tanto respecto al tipo básico como a los subtipos agravados, *cuando los hechos se hubieran cometido mediante la utilización ilícita de datos personales de otra persona para facilitarse el acceso informático o para ganarse la confianza de un tercero.*

La incorporación de esta agravación en los delitos contra los datos y programas informáticos y documentos electrónicos ajenos responde a los parámetros de la Directiva 2013/40/UE que, en su considerando decimocuarto, llama la atención sobre la conveniencia de establecer *medidas eficaces contra la usurpación de identidad y otras infracciones relacionadas con la identidad y* que incluye esta circunstancia, en su art. 9-5º, como una de las que ha de ser tenida en cuenta para la agravación de las penas por los ilícitos que nos ocupan.

El Legislador no ha incorporado la agravante de forma exacta a como se configura en la Directiva. Recordemos que en el art. 9.5 de aquella la circunstancia se concreta en la comisión de la infracción *utilizando ilícitamente datos de carácter personal de otra persona con la finalidad de ganar la confianza de un tercero, causando así daños al propietario legítimo de la identidad.* Sin embargo, en nuestro ordenamiento la aplicación de esta circunstancia se hace depender de la utilización ilícita de dichos datos para facilitarse el acceso al sistema o para ganarse la confianza de un tercero.

Obsérvese en primer término que en estos delitos la circunstancia se integra por la utilización de datos de carácter personal de cualquier persona - que por la dicción de precepto hay que entender como realmente existente - y no exclusivamente los de la propia víctima del delito, como ocurre en el supuesto del art. 197.4, lo cual posibilita un marco mucho más amplio de aplicación de esta circunstancia. Dicha utilización ha de ser ilícita, es decir, no autorizada ni consentida por el titular de la identidad suplantada. Respecto al alcance del concepto de *datos personales*, debe atenderse al análisis efectuado anteriormente a propósito de la aplicación de la circunstancia similar en los delitos de descubrimiento y revelación de secretos (apartado 1.1 B)

En cuanto a los restantes requisitos, el texto legal omite acertadamente la exigencia, que establece la Directiva, de que se cause un perjuicio al titular de la identidad usurpada, extremo que parece incongruente en este contexto teniendo en cuenta los bienes jurídicos protegidos. En cualquier caso, dicho resultado pudiera quedar amparado por otros preceptos penales y dar lugar la correspondiente indemnización civil. Sin embargo, en sentido contrario, el legislador español ha decidido ampliar el ámbito de aplicación de la agravación haciéndola extensiva también a los supuestos en los que el uso de datos personales ajenos tiene por objetivo *facilitarse el acceso al sistema informático*, circunstancia ésta especialmente adecuada en atención a la naturaleza de las conductas ilícitas a las que es aplicable.

En todo caso, la finalidad del uso irregular de los datos personales de otro es el de servir de medio para la ejecución de la acción típica prevista en el apartado primero del precepto examinado, bien sea haciendo posible el acceso al sistema objeto de ataque o para conseguir la confianza de un tercero que, a su vez, favorezca o facilite la causación de daños en los elementos del sistema.

2.2 El nuevo art. 264 bis CP.

Como ya se ha indicado, la LO 1/2015, siguiendo también en este punto el criterio de la Directiva europea, aborda en preceptos separados la descripción y sanción de las acciones ilícitas contra datos, programas informáticos y documentos electrónicos ajenos y aquellas otras cuyo objeto son los sistemas, en sí mismos considerados, como conjunto interconectado de elementos informáticos. Por ello y en referencia a estas últimas articula un nuevo precepto cuyo tenor es el siguiente:

1. Será castigado con la pena de prisión de seis meses a tres años el que, sin estar autorizado y de manera grave, obstaculizara o interrumpiera el funcionamiento de un sistema informático ajeno:

a) realizando alguna de las conductas a que se refiere el artículo anterior;
b) introduciendo o transmitiendo datos; o
c) destruyendo, dañando, inutilizando, eliminando o sustituyendo un sistema informático, telemático o de almacenamiento de información electrónica.

Si los hechos hubieran perjudicado de forma relevante la actividad normal de una empresa, negocio o de una Administración pública, se impondrá la pena en su mitad superior, pudiéndose alcanzar la pena superior en grado.

2. Se impondrá una pena de prisión de tres a ocho años y multa del triplo al décuplo del perjuicio ocasionado, cuando en los hechos a que se refiere el apartado anterior hubiera concurrido alguna de las circunstancias del apartado 2 del artículo anterior.

3. Las penas previstas en los apartados anteriores se impondrán, en sus respectivos casos, en su mitad superior, cuando los hechos se hubieran cometido

mediante la utilización ilícita de datos personales de otra persona para facilitarse el acceso al sistema informático o para ganarse la confianza de un tercero.

También en este caso, y a efectos de facilitar la exégesis del nuevo precepto, resulta de interés traer a colación la regulación que hace la Directiva europea de esta materia y que se recoge en su art. 4 en estos términos: *Los Estados miembros adoptarán las medidas necesarias para que la obstaculización o la interrupción significativas del funcionamiento de un sistema de información, introduciendo, transmitiendo, dañando, borrando, deteriorando, alterando, suprimiendo, o haciendo inaccesibles datos informáticos, intencionadamente y sin autorización, sea sancionable como infracción penal, al menos en los supuestos que no sean de menor gravedad*

El Legislador ha optado por definir de forma muy abierta, e incluso reiterativa, la conducta típica que consiste básicamente en lograr un resultado concreto, cual es la obstaculización o interrupción de la normal actividad de un sistema informático ajeno, de manera grave y a través de alguna de las acciones indicadas en el precepto.

Se trata, por tanto, de un delito de resultado en el que el elemento esencial es que se produzca la efectiva y grave obstaculización o interrupción respecto de un sistema informático concreto. Por sistema informático debe entenderse, a tenor de la Directiva 2013/40/UE, que sigue el criterio de la Decisión Marco precedente, *todo aparato o grupo de aparatos interconectados o relacionados entre sí, uno o varios de los cuales realizan, mediante un programa, el tratamiento automático de datos informáticos, así como los datos informáticos almacenados, tratados, recuperados o transmitidos por estos últimos para su funcionamiento, utilización, protección y mantenimiento*.

En cuanto a la interpretación del término grave, que cualifica la interrupción/obstaculización del sistema, resulta también de interés acudir a la

terminología empleada en el texto original de la propia Directiva que utiliza a dicho fin la expresión *seriously* (seriamente) en referencia al alcance de la interferencia. Quiere decirse con ello que no toda obstaculización o interrupción del funcionamiento de un sistema informático se haría acreedora por si sola de una sanción penal, sino únicamente aquella que afectara realmente y de forma significativa la funcionalidad del sistema atacado, circunstancia que será necesario analizar en cada supuesto en particular y que, en un buen número de ocasiones, precisará de los correspondientes informes técnicos.

El texto que se examina, al igual que el del art. 264, en su versión inicial y en la derivada de la reforma, acota la conducta típica con el requisito, no contemplado en la Directiva, de que el sistema informático, o en su caso los datos, programas o documentos electrónicos, sean ajenos. Este requisito resulta sin duda perturbador por la dificultad de concretar qué ha de entenderse por ajenidad en referencia no ya a objetos físicos sino a elementos de carácter inmaterial, concebidos para operar y ser utilizados en un entorno virtual en muchas ocasiones diseñado con el objetivo específico de compartir información y gestionarla para su mejor aprovechamiento colectivo. Ciertamente habrá supuestos en que esa ajenidad resulte incuestionable, como aquellos en los que la agresión provenga de un agente completamente externo, pero en muchos supuestos el origen del ataque puede estar en la acción ilícita de personas o colectivos que interactúan o son usuarios del propio sistema y a dicho fin incorporan o comparten información a través del mismo. En estos casos acreditar el requisito de la ajenidad puede entrañar dificultades. Por esta razón dicho elemento habrá de integrarse e interpretarse conjuntamente con el de la falta de autorización o, dicho de otra forma, con la falta de disponibilidad de los contenidos o del sistema sobre el que se actúa; de tal forma que serían típicas aquellas acciones que se realizan intencionadamente sobre los mismos, con los objetivos indicados, sin estar habilitado para ello. En consecuencia, solo la actuación no necesitada de autorización sobre sistemas informáticos propios, respecto de los cuales su titular tiene pleno control y disposición, quedarían al margen de la aplicación de este precepto.

El Legislador español dedica tres apartados a describir las conductas típicas a través de la cuales se pretende lograr el resultado de obstaculizar o interrumpir el normal funcionamiento de un sistema informático. En el primer apartado incluye todos los comportamientos del art. 264.1 CP: borrar, dañar, deteriorar, alterar, suprimir, o hacer inaccesibles datos, programas informáticos o documentos electrónicos ajenos. Es decir cuando a través de las indicadas acciones el efecto que se pretende y se produce afecta no solo a los elementos aislados que integran el sistema sino que incide en la operatividad funcional del sistema de información mismo.

En el segundo apartado el precepto incluye las conductas de transmitir o introducir nuevos datos en el sistema, que habrán de entenderse referidas a aquellas que, no estando comprendidas en la relación recogida en el apartado anterior, puedan también causar como efecto la interrupción u obstaculización del funcionamiento del sistema. En realidad la acción de *alterar* datos, programas o documentos recogida en el art. 264.1º puede llevarse a efecto introduciendo nuevos datos, por lo que muchos de estos comportamientos pudieran ser reconducidos al apartado anterior. El ejemplo más característico de este tipo de actuaciones son los ataques de denegación de servicio, conocidos vulgarmente como DDoS (*Distributed Denial of Service*).

Finalmente, en el tercero de los apartados, se relacionan los comportamientos de destruir, dañar, inutilizar, eliminar o sustituir pero dirigidos directamente y en su conjunto al sistema de información o de almacenamiento masivo afectados por la acción ilícita.

Como puede constatarse, muchas de las conductas que contempla el art. 264 bis son reconducibles a las acciones típicas sancionadas en el art. 264. 1 CP, por lo que en una pluralidad de ocasiones la aplicación de una u otra figura típica vendrá

determinada por la capacidad de la acción ilícita para afectar a la operatividad del sistema informático en su conjunto.

El párrafo segundo del apartado primero del art. 264 bis CP establece la imposición de la pena en su mitad superior, que incluso podrá elevarse hasta el grado superior, cuando la interrupción u obstaculización grave del sistema informático haya tenido como consecuencia un perjuicio relevante en la empresa, negocio u organismo de la Administración Pública al que - según ha de entenderse - sirve el sistema afectado. Esta circunstancia, obviamente, deberá acreditarse en cada supuesto y la mayor o menor relevancia del perjuicio dependerá del tipo de actividad y de la entidad de la empresa, organismo o institución de que se trate.

A su vez, el apartado segundo del mismo precepto hace extensivos los subtipos agravados del art. 264 a las acciones ilícitas contra los sistemas informáticos, por lo que debe hacerse una remisión a las reflexiones efectuadas al respecto al comentar el citado precepto, en el apartado 2.1.1. de esta misma Circular. Únicamente debe reseñarse la diferencia penológica entre ambos supuestos, ya que en el art. 264 CP la sanción privativa de libertad prevista para estos subtipos es de dos a cinco años y multa del tanto al decuplo del perjuicio causado, con posibilidad de elevarse en grado si es apreciable extrema gravedad, en tanto que en el art. 264 bis el marco de la pena privativa de libertad es de tres a ocho años y multa del triplo al decuplo del perjuicio causado.

Es evidente, por tanto, que el Legislador ha considerado notablemente más graves y peligrosas - porque así lo son efectivamente - las acciones dirigidas contra el sistema informático en su conjunto que provocan su interrupción u obstaculizan de forma grave su normal funcionamiento, respecto de aquellas otras que afectan exclusivamente a los datos, programas o documentos electrónicos aun cuando tengan incidencia, al menos indirecta, en el sistema en el que se integran, siempre que no impliquen una pérdida significativa en la funcionalidad del mismo.

Para finalizar el análisis de este precepto se ha de indicar que, conforme a lo dispuesto en el apartado tercero del mismo, también en estos supuestos, se contempla como circunstancia agravante y en iguales términos que en el art. 264.3 CP, *la utilización ilícita de datos personales de otra persona para facilitarse el acceso al sistema informático o para ganarse la confianza de un tercero,* por lo que son trasladables los comentarios efectuados al respecto en el apartado 2.1.2 de este documento.

2.3 El nuevo art. 264 ter CP.

La redacción del precepto es la siguiente:

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 dos art.s anteriores:

a) un programa informático, concebido o adaptado principalmente para cometer alguno de los delitos a que se refieren los dos artículos anteriores; o
b) una contraseña de ordenador, un código de acceso o datos similares que permitan acceder a la totalidad o a una parte de un sistema de información.

Se trata de un precepto de contenido idéntico al del art. 197 ter, analizado en el marco de los delitos de descubrimiento y revelación de secretos, si bien en este supuesto, y a diferencia de aquellos, la persecución de estas conductas no está sujeta a condiciones especiales de procedibilidad.

La redacción de este precepto deriva directamente del art. 7 de la Directiva 2013/40/UE sobre ataques a los sistemas de información y, como aquél, sanciona la producción, adquisición para propio uso, importación o facilitación a terceros, sin estar autorizado para ello, de las herramientas o instrumentos reseñados en los

apartados a) y b) con la intención de facilitar las acciones ilícitas contra datos, programas informáticos, documentos electrónicos o sistemas informáticos contempladas en los artículos 264 y 264 bis.

En los últimos años es cada vez más frecuente detectar programas o herramientas informáticas preparadas específicamente para alterar, dañar o destruir datos o programas informáticos u obstaculizar o interrumpir el normal funcionamiento de un sistema, de tal modo que su única utilidad es precisamente llevar a efecto esas acciones ilícitas. Entre ellos ha sido tristemente célebre, precisamente porque su utilización ha afectado a muchas personas, el conocido como *ransonware* que puede ser utilizado para cifrar archivos concretos o también la totalidad del contenido del sistema informático infectado. Una de sus últimas versiones, *Cryptolocker,* encripta todo los documentos y archivos del sistema expandiendo sus efectos hasta la unidades de red y las copias de seguridad por lo que el perjuicio causado a la víctima por la pérdida total de información puede llegar a tener consecuencias muy graves.

Pues bien, la realización de las conductas típicas a efectos de obtener o facilitar a otros la disponibilidad de estos programas, así como también de contraseñas de ordenador, códigos de acceso o datos que permitan el acceso a la totalidad o a una parte de un sistema informático, integrará esta conducta cuando quien así actúe no se encuentre debidamente autorizado para ello y, además se acredite la intención de destinarlos a la comisión de cualquiera de las conductas de daños informáticos anteriormente examinadas.

Conclusiones

Delitos de descubrimiento y revelación de secretos
Nueva circunstancia agravatoria del art. 197.4º b) CP

1ª Se incorpora, en el art. 197.4º b), una nueva circunstancia agravatoria cuando los hechos sancionados en los párrafos 1º y 2º del mismo art. *se lleven a cabo mediante la utilización no autorizada de datos personales de la víctima.*

A estos efectos por datos personales habrían de entenderse no solo los datos de identidad oficial, en sentido estricto, sino cualesquiera otros, propios de una persona o utilizados por ella, que le identifiquen o hagan posible su identificación frente a terceros tanto en un entorno físico como virtual. Tienen tal consideración no solo el nombre y apellidos, sino también, entre otros, los números de identificación personal como el correspondiente al DNI, el de afiliación a la Seguridad Social o a cualquier institución u organismo público o privado, el número de teléfono asociado a un concreto titular**,** la dirección postal, el apartado de correos, la dirección de correo electrónico, la dirección IP, la contraseña/usuario de carácter personal, la matrícula del propio vehículo, las imágenes de una persona obtenidas por videovigilancia, los datos biométricos y datos de ADN, los seudónimos y en general cualquier dato identificativo que el afectado utilice habitualmente y por el que sea conocido.

Nueva figura delictiva del art. 197.7 CP.

2ª El delito del art. 197.7 CP sanciona penalmente la divulgación a terceros de imágenes o grabaciones audiovisuales de una persona que**,** aun obtenidas con su consentimiento, se difunden, revelan o ceden sin su anuencia, lesionando gravemente su intimidad personal. Por tales habrá que entender tanto los contenidos perceptibles únicamente por la vista, como los que se perciben conjuntamente por el oído y la vista y también aquellos otros que, aun no mediando imágenes, pueden captarse por el sentido auditivo.

3ª El precepto es aplicable cuando la imagen o grabación, posteriormente difundida, se haya tomado en un ámbito espacial reservado, circunstancia ésta que el tipo penal concreta en la exigencia de que se haya obtenido en un domicilio o en

un lugar fuera del alcance de la mirada de terceros. Por tal habrá de entenderse cualquier lugar cerrado o también un lugar al aire libre si se acredita que reúne garantías suficientes de privacidad para asegurar que la captación de las escenas/imágenes se efectuó en un contexto de estricta intimidad sustraído a la percepción de terceros ajenos a ellas.

4ª El requisito de falta de autorización del afectado no exige acreditar una negativa expresa sino que bastará con la no constancia de autorización, a la que han de equipararse los supuestos de falta de conocimiento de la ulterior cesión o distribución por parte del afectado. Si fueran varias las personas que aparecen en las imágenes la difusión solo resultará atípica si hubieran accedido a la difusión todas y cada una de ellas.

5ª Al configurarse como un delito especial propio**,** incurre en responsabilidad únicamente quien, habiendo obtenido con anuencia de la víctima la imagen o grabación, inicia la cadena de difusión consciente de que carece de autorización para ello del propio afectado y por tanto de que su conducta lesiona la intimidad de la víctima. Ello sin perjuicio de la responsabilidad exigible en los supuestos de coparticipación criminal por coautoría, cooperación necesaria, inducción o complicidad, si concurren los presupuestos previstos en los artículos 28 y 29 CP.

Al margen de dichos supuestos, quien, sin haber participado en la obtención de la imagen o grabación, la trasmite posteriormente a terceros a sabiendas de su contenido y de la falta de autorización de la víctima -*extranei*- podría incurrir en un delito contra la integridad moral del articulo 173.1 CP, si concurren los requisitos de dicho tipo penal y concretamente cuando dicha difusión menoscabe gravemente la integridad moral de la persona afectada.

6ª El autor del delito del art. 197.7 podría incurrir también en un delito contra la integridad moral del art. 173.1 del CP cuando la difusión inconsentida lesione no solo la intimidad del afectado sino también, por la naturaleza de las imágenes difundidas, afecte gravemente a la integridad moral de la víctima. En estos supuestos será de apreciación un concurso ideal entre ambos delitos a penar de conformidad con el artículo 77.2 del mismo texto legal.

7ª Cuando las imágenes obtenidas y posteriormente difundidas se refieran a un menor o a una persona con discapacidad y merezcan la consideración de material pornográfico, tal y como de se define en el art. 189 del CP, se plantea una situación de concurso entre la figura prevista en el 197.7 y los preceptos correspondientes a los delitos de pornografía infantil.

En estos supuestos se produciría un concurso ideal entre el delito que se examina, art. 197.7, párrafo 2º y el art. 189.1º b) ambos del CP, a penar de conformidad con el art. 77.2 del mismo texto legal dado que la acción ilícita, no solamente lesiona la intimidad del afectado cuya imagen se difunde sin su autorización, sino que pone también en peligro la indemnidad sexual de los menores, genéricamente considerados, como bien jurídico protegido en los delitos de pornografía infantil.

El delito de acceso ilegal a sistemas informáticos (art. 197 bis 1º)

8ª La reubicación sistemática de esta figura delictiva en el art. 197 bis 1º del CP deja constancia de que el bien jurídico protegido en el mismo, no es directamente la intimidad personal, sino más bien la seguridad de los sistemas de información en cuanto medida de protección del ámbito de privacidad reservado a la posibilidad de conocimiento público. El delito se consuma por el mero hecho de acceder - o facilitar a otro el acceso- a un sistema informático o a parte del mismo aun cuando la acción no vaya seguida del apoderamiento de datos, informaciones o documentos ajenos.

Por medida de seguridad ha de entenderse cualquiera que se haya establecido con la finalidad de impedir el acceso al sistema, con independencia de que la misma sea más o menos sólida, compleja o robusta y también de que haya sido establecida por el administrador, el usuario, o por el instalador del sistema siempre que se mantenga operativa como tal medida de seguridad por quien está legitimado para evitar el acceso.

9ª En la práctica será frecuente la concurrencia de este tipo, acceso ilegal a sistemas, con cualquiera de las conductas previstas en el artículo 197 nº 1 y 2. En estos casos, en términos generales, será de apreciar un concurso medial del artículo 77 CP, al igual que en los supuestos en que el acceso ilegal tuviera por objeto el descubrimiento de secretos de empresa (art 278 CP) o el descubrimiento de secretos oficiales (art. 598 y ss CP). Ello no obsta a que en casos concretos, en los que no sea posible el acceso a la información íntima o a los datos personales por medio distinto que la vulneración de medidas de seguridad del sistema, pudiera considerarse la posibilidad de apreciar una progresión delictiva que llevaría a considerar el concurso de normas sancionable por la vía del artículo 8.3 CP

En todo caso, cuando para sortear las medidas de seguridad fuera preciso utilizar datos de carácter personal de la víctima, la apreciación del art. 197 bis 1º junto con el artículo 197, 4 b) supondría una infracción del principio *non bis in idem*, debiendo aplicarse en estos casos este último precepto, por mor del principio de especialidad establecido en el artículo 8.1 del CP.

El delito de interceptación ilegal de datos informáticos (art 197 bis 2º)

10ª El objeto de protección en este tipo penal es doble. En primer término lo son los datos informáticos objeto de cualquier tipo de transmisión -salvo las tengan el carácter de comunicación personal cuya interceptación se sanciona en el art 197.1º- que se lleve a efecto, incluso sin necesidad de intervención humana, entre los distintos dispositivos de un sistema o entre dos o más sistemas y en forma no

pública, es decir en condiciones tales que dichos datos queden excluidos del conocimiento de terceros. En segundo término se protegen también los datos informáticos de un sistema que son susceptibles de obtenerse a partir de las emisiones electromagnéticas del mismo.

En uno y otro caso, para que la conducta sea delictiva han de concurrir dos requisitos: que quien efectúa la interceptación no esté autorizado para ello y que la misma se realice utilizando como medio artificios o instrumentos técnicos, debiendo entenderse por tales cualesquiera herramientas o mecanismos que hagan posible este objetivo aunque no estén específicamente destinados a ello.

11ª La ubicación de este delito en el nuevo art. 197 bis. 2º, junto al acceso ilegal a sistemas informáticos, es coherente con la voluntad del legislador de separar la tipificación y sanción de las conductas que tutelan la privacidad protegiendo la seguridad de los sistemas de aquellas otras en las que el bien jurídico protegido es directamente la intimidad de las personas. En los supuestos de concurrencia entre la interceptación ilegal del artículo 197 bis 2º y los delitos del artículo 197.1º, el criterio a aplicar será el del concurso de normas a resolver conforme al principio de absorción dado que uno de los comportamientos típicos que reseña el último precepto citado es el de interceptar las comunicaciones o utilizar artificios técnicos de escucha, transmisión, grabación o reproducción de imágenes, sonidos o cualquier otra señal de comunicación, por lo que entraría en juego el artículo 8.3º CP a cuyo tenor *el precepto legal más amplio o complejo absorberá a los que castiguen las infracciones consumidas en aquel*, siendo de aplicación por tanto el artículo 197.1º

Ahora bien, en el supuesto de que la interceptación ilegal que estamos examinando (art 197 bis 2º) concurra con alguna de las conductas ilícitas contempladas en el art. 197.2º habrá de apreciarse un concurso medial, del art 77 CP por las mismas razones y con las salvedades expuestas anteriormente a propósito de la concurrencia del artículo 197 bis 1º con esta misma conducta.

El delito de abuso de dispositivos (art. 197 ter)

12ª La utilización de los verbos producir, adquirir para el uso, importar o de cualquier modo facilitar a tercero en la definición de la conducta típica lleva a entender incluidas en la misma tanto la elaboración para uso propio, o para distribución a terceros, como la importación, la adquisición y en consecuencia la ulterior posesión -aunque el precepto no lo indique expresamente- bien sea para el propio uso o para la distribución o entrega a otro u otros y en general cualquier forma de puesta a disposición de terceros de cualquiera de las herramientas o instrumentos que se relacionan en los apartados a) y b) del mismo precepto.

Dichos instrumentos y herramientas pueden ser: programas informáticos y/o contraseñas, códigos de acceso o datos similares que hagan posible el acceso a un sistema. Respecto a los primeros la exigencia legal de que se trate de programas *concebidos o adaptados principalmente* para cometer determinados delitos remite al software malicioso o *malware* diseñado para infiltrarse y/o obtener información (programas espía) en un dispositivo o un sistema de información sin el consentimiento de su propietario, quedando excluidos cualquier otro tipo de programas que no reúnan dicha característica, aunque puedan ocasionalmente servir para esa misma finalidad, circunstancia cuya determinación hará necesario generalmente un informe pericial.

Por su parte, la referencia a contraseñas, códigos o datos similares, concierne a medidas de seguridad instaladas para evitar la intromisión en archivos, partes de un sistema o en el sistema mismo por quien no se encuentra habilitado para ello. No estamos por tanto ante herramientas elaboradas específicamente para hacer posible la intromisión ilegítima en un sistema sino ante la irregular disponibilidad de las legítimamente creadas y utilizadas para impedir dicha intromisión.

13ª La posibilidad de actuar penalmente ante dichos comportamientos se encuentra acotada por dos elementos, la falta de autorización para la elaboración, importación, adquisición o facilitación a terceros de esos instrumentos o herramientas y la exigencia de que dichas acciones estén orientadas a *facilitar la comisión de alguno de los delitos a que se refieren* los artículos 197, 1º y 2º y 197 bis CP. En consecuencia es imprescindible que quien así actúa no cuente con autorización, bien sea otorgada legalmente bien porque se le haya encomendado dicha responsabilidad por quien tenga capacidad para ello en el marco concreto de la actividad de que se trate. Pero además ha de actuarse con la finalidad específica de facilitar la comisión de uno de los delitos mencionados, circunstancia que habrá de acreditarse en cada supuesto, atendiendo a los elementos, pruebas o indicios existentes.

14ª Cuando quien haya producido, importado o adquirido estas herramientas o instrumentos sea el mismo que posteriormente comete el delito concreto, bien sea del art. 197 apartados 1 y 2) o del art. 197 bis, utilizando esos mismos medios fabricados, adquiridos o poseídos a dicho fin, habrá de entenderse que se produce un concurso de normas, a resolver de acuerdo con el criterio de absorción previsto en el art. 8.3 del CP.

La agravación del art. 197 quater

15ª La LO 1/2015 traslada a este precepto la agravación derivada de la comisión del hecho en el seno de una organización o grupo criminal, anteriormente sancionada en al art 197.8, haciéndola extensiva a todos los delitos descritos en Capítulo I del Título X del Libro II del CP.

En estas ocasiones, cuando el sujeto activo de cualquiera de los delitos de descubrimiento y revelación de secretos sea, al tiempo, integrante y/o dirigente del grupo u organización participante en la acción ilícita se produce un concurso de normas con los arts. 570 bis o 570 ter del CP. Ha de recordarse, por tanto, el

criterio establecido en la Circular 2/2011 que, en aplicación de lo establecido en art. 570 quáter in fine, remite en estos casos al art 8.4 CP y, por tanto, establece que *en tales supuestos los Sres Fiscales cuidarán de aplicar, de acuerdo con lo dispuesto en el art 570 quater CP, conforme al criterio de alternatividad, un concurso de delitos entre el art. 570 bis o el art. 570 ter, en su caso y el tipo correspondiente al delito específicamente cometido con todas sus circunstancias si bien prescindiendo de la agravación específica de organización, cuando la pena así aplicada sea superior a la que prevé el subtipo agravado.*

Condiciones de perseguibilidad

16ª La ubicación de los nuevos tipos penales determina que les sea de aplicación la previsión del art. 201 CP a cuyo tenor *para proceder por los delitos previstos en este capítulo será necesaria denuncia de la persona agraviada o de su representante legal,* sin perjuicio de las facultades asignadas al Ministerio Fiscal cuando se trate de personas menores de edad o en situación de discapacidad. Esta exigencia puede dificultar la aplicación de estos preceptos, especialmente del art. 197 ter, dado que tipifica actos preparatorios del ataque informático en los que no es necesario que la conducta ejecutada haya llegado a *agraviar* a personas determinadas.

No obstante, a estos efectos, ha de tenerse en cuenta la previsión del art. 201.2 que hace innecesaria dicha denuncia si el delito afecta a intereses generales o a una pluralidad de personas. Esta circunstancia se valorará en atención al número o características del sistema o sistemas informáticos objeto de acceso o interceptación ilegal y, en los supuestos del art. 197 ter, cuando la concreción en el curso de la investigación del fin a que se destinaban las herramientas o instrumentos permita dicha conclusión, por ejemplo cuando el objeto de la acción fuera el espionaje informático de organismos e instituciones del Estado o cuando lo que se pretenda sea la obtención masiva de credenciales bancarias o acciones de similar naturaleza planificadas para afectar a muchas personas.

Delitos de daños informáticos

El delito de daños en datos, programas informáticos o documentos electrónicos. (Art 264)

17ª En referencia a la circunstancia prevista en el art. 264.2.2º CP, la conjunción disyuntiva que enlaza las circunstancias de ocasionar daños de especial gravedad *o* afectar a un número elevado de sistemas ha de interpretarse en el sentido de que no es necesario que ambas concurran conjuntamente sino que es posible aplicar la agravación aun cuando solo sea apreciable una u otra de dichas circunstancias.

La interpretación de los conceptos de *gravedad y especial gravedad* del daño causado, por su carácter indeterminado y su dificultad de concreción -dada la naturaleza inmaterial de los elementos afectados - hace necesaria una labor exegética que deberá llevarse a efecto a partir de la doctrina jurisprudencial sobre supuestos concretos. Sin perjuicio de ello, y de conformidad con los parámetros fijados por la Directiva 40/2013/UE, habrían de considerarse graves, y por tanto encuadrables por su resultado en el art. 264.1 CP, todas aquellas acciones ilícitas que tuvieran trascendencia significativa o generaran consecuencias apreciables en datos, programas informáticos o documentos electrónicos o en los intereses en juego, quedando la aplicación del subtipo que nos ocupa para los supuestos en que los efectos del delito fueran especialmente relevantes y no se hicieran merecedores, por su especial intensidad, de la calificación de extrema gravedad

La circunstancia prevista en el inciso segundo del art. 264.2.2º CP habrá de aplicarse específicamente en los supuestos en los que se encuentre afectado un número tal de sistemas de información que pueda considerarse la existencia de un ataque informático masivo en el sentido a que se refiere el cuerpo de esta Circular.

18ª La circunstancia del art. 264.2.3ª será aplicable cuando el ataque informático a datos, programas o documentos electrónicos afecte gravemente a la prestación ordinaria de servicios esenciales o a la provisión de bienes de primera necesidad. A estos efectos se entienden por servicios esenciales aquellas actividades que sirven para el mantenimiento de las funciones sociales básicas de la comunidad, como la salud, la seguridad, la protección de los derechos fundamentales y las libertades públicas y el normal funcionamiento de las Instituciones del Estado. En cuanto a los bienes de primera necesidad deben considerarse como tales los alimentos, medicamentos y otros productos de consumo imprescindible para la subsistencia y salud de las personas.

19ª La agravación del art. 264.2.4ª operará con la simple afección al sistema informático de una infraestructura crítica, definida como tal en el CP, sin que sea necesario para ello que los efectos en los datos o programas informáticos o en el propio sistema sea de carácter grave. En cuanto a la creación de una situación de peligro para la seguridad del Estado, de la Unión Europea o de un Estado Miembro de la Unión Europea, la agravación solo será apreciable si el riesgo creado ha sido efectivamente grave.

20ª La agravación específica prevista en el apartado 3º del art. 264 establece, de forma preceptiva, la imposición de las penas en su mitad superior, tanto respecto al tipo básico como en los subtipos agravados. La circunstancia se integra por la utilización no autorizada de datos personales de cualquier otra persona -que hay que entender como realmente existente- como medio para facilitar el acceso al sistema objeto de ataque o para conseguir la confianza de un tercero que, a su vez, favorezca o facilite la causación de daños en los elementos del sistema.

Respecto al alcance del concepto *datos personales*, los Sres. Fiscales tomarán en consideración el análisis efectuado anteriormente a propósito de la aplicación de la circunstancia similar en los delitos de descubrimiento y revelación de secretos (conclusión primera).

21ª Todas las conductas ilícitas de los arts. 197 bis, 197 ter y 264 a 264 ter pueden integrar el delito de terrorismo del art. 573.2 si se llevan a efecto con cualquiera de las finalidades previstas en el art. 573.1 CP, siendo más evidente esta posibilidad cuando concurran algunos de los subtipos agravados del art. 264.2 CP. En estos casos se produce un concurso de normas a resolver por el principio de especialidad recogido en el art. 8.1º y en el propio art. 573.2. Ello no solamente incide en la calificación jurídica del hecho sino también en la determinación de la competencia objetiva al estar atribuido el conocimiento de esas tipologías delictivas a los órganos de la Audiencia Nacional.

El delito de obstaculización o interrupción del funcionamiento de sistemas informáticos (art. 264 bis)

22ª El art. 264 bis CP sanciona un delito de resultado consistente en la obstaculización o interrupción del funcionamiento de un sistema informático ajeno, sin estar autorizado y de manera grave, a través de alguna de las acciones indicadas en el apartado primero del mismo precepto.

El término *grave* ha de interpretarse en el sentido de que no toda obstaculización o interrupción del funcionamiento de un sistema se haría acreedora por si sola de una sanción penal sino únicamente aquella que afecte realmente y de forma significativa a la funcionalidad del sistema atacado, circunstancia que será necesario analizar en cada supuesto en particular y que en un buen número de ocasiones precisará de los correspondientes informes técnicos.

23ª El carácter *ajeno* de los sistemas informáticos objeto del delito ha de integrarse e interpretarse conjuntamente con el requisito de la falta de autorización o, dicho de otra forma, con la falta de disponibilidad de los contenidos o del sistema sobre el que se actúa; de tal forma que serían típicas aquellas acciones que se realizan intencionadamente sobre los mismos, con los objetivos indicados, sin estar

habilitado para ello. En consecuencia, solo la actuación no necesitada de autorización sobre sistemas informáticos, respecto de los cuales su titular tiene pleno control y disposición, quedaría al margen de la aplicación de este precepto.

24ª El precepto agrupa en tres apartados las conductas típicas a través de las cuales se pretende el resultado de obstaculizar o interrumpir el funcionamiento de un sistema informático. En el primer apartado incluye todas las relacionadas en el art. 264.1º CP, que integrarán el delito del art. 264 bis cuando el efecto que se pretende y produce incide no solo en los elementos que integran el sistema sino que afecta a la operatividad del sistema de información mismo.

En el apartado b) se sanciona la transmisión e introducción de nuevos datos, cuando dichas conductas no se encuentren comprendidas en el apartado anterior y sean susceptibles de causar como efecto la interrupción u obstaculización del funcionamiento del sistema.

Finalmente en el apartado c) se relacionan los comportamientos de destruir, dañar, inutilizar, eliminar o sustituir pero dirigidos directamente y en su conjunto al sistema de información o de almacenamiento masivo afectados por la acción ilícita.

Muchos de estos comportamientos son reconducibles a las acciones típicas sancionadas en el art. 264.1º CP por lo que en una pluralidad de ocasiones la aplicación de uno u otro tipo penal vendrá determinada por la capacidad de la acción para afectar a la operativad o al funcionamiento del sistema informático en su conjunto.

El delito de abuso de dispositivos (art. 264 ter)

25ª El tipo penal presenta idéntico contenido al del art. 197 ter, analizado en el marco de los delitos de descubrimiento y revelación de secretos (conclusiones decimosegunda a decimocuarta) si bien en este supuesto los programas

informáticos producidos, adquiridos para su uso, importados o facilitados a terceros han de estar concebidos o adaptados principalmente para la comisión de algunos de los delitos sancionados en los arts. 264 y 264 bis, al igual que las conductas típicas han de ejecutarse con esa misma finalidad. No obstante en estos supuestos, y a diferencia de aquellos, la persecución de estas conductas no está sujeta a condiciones especiales de procedibilidad.

En razón de todo lo expuesto, los Sres. Fiscales se atendrán en lo sucesivo a las prescripciones de la presente Circular.

Madrid, 21 de septiembre de 2017
EL FISCAL GENERAL DEL ESTADO

José Manuel Maza Martín

EXCMOS./AS. E ILMOS./AS. SRES./AS. FISCALES DE SALA, FISCALES SUPERIORES, FISCALES JEFES PROVINCIALES Y DE ÁREA.