7.1 **Circulares, Consultas e Instrucciones**

Durante el ejercicio correspondiente al año 2017, se han elaborado los borradores de los siguientes documentos:

– *Circular 1/2017, sobre la interpretación del art. 183 quater del Código Penal*

Obedece esta circular a la necesidad de fijar un criterio interpretativo acorde con la nueva regulación, conforme a la cual el consentimiento libre del menor de dieciséis años excluirá la responsabilidad por posibles delitos de abusos y agresión sexual cometidos sobre los menores de esta edad, y cuando tal consentimiento tendrá la relevancia suficiente para excluir una posible responsabilidad penal.

Se considera que el fundamento de la excepción contemplada en el art. 183 quater CP radica en evitar interpretaciones estrictas que castiguen las relaciones sexuales consentidas entre adolescentes o personas jóvenes entre las que no existan diferencias sustanciales en cuanto edad y madurez. Dicha situación excluye la noción de abuso. Así, se estima que el Legislador, para conferir eficacia al consentimiento del menor de 16 años, ha optado por un criterio mixto fundado en dos parámetros: uno cronológico (edad similar) y otro biopsicosocial (semejante grado de desarrollo o madurez).

El art. 183 quater no define franjas concretas de edad. Es posible, no obstante, fijar marcos de protección según la víctima sea impúber (en todo caso), haya alcanzado la pubertad y no sea mayor de 13 años (la exención se limitaría generalmente a autores menores de 18 años), y menores de 14 y 15 años (cuyos contactos sexuales podrían abarcar a sus iguales jóvenes). Dentro de la franja de edad de los adultos jóvenes, debe precisarse entre la comprendida entre 18 y menos de 21 y la situada entre 21 y 24 años inclusive. En la última subdivisión, solo muy excepcionalmente, podrá contemplarse la exclusión o la atenuación habida cuenta de la importante diferencia de edad y el alejamiento de las franjas cronológicas que, ordinariamente, resultan del derecho comparado (entre 2 y 5 años). Se recalca, en cualquier caso, que estos criterios deben considerarse orientadores.

La capacidad de comprender y evaluar las consecuencias de los actos no va ligada, de manera uniforme, a la edad cronológica. Las diferencias en este aspecto deben constatarse caso por caso y, sobre todo atender al hecho de que, cuanto mayor sea la diferencia de edad, mayor necesidad habrá de acreditar la semejanza en cuanto a desarrollo o madurez.

En lo que atañe a la LORPM, siguen manteniendo su vigencia, *mutatis mutandis*, los pronunciamientos de la Circular 9/2011, de 16 de noviembre. Debiéndose buscar la respuesta individualizada en cada caso, que puede ser el archivo (art. 16 LORPM), cuando por las circunstancias y proximidad de edad se estime que los hechos no afectan ni a la libertad ni a la indemnidad sexual y quedan al margen del ámbito de protección de la norma penal.

Cabe la posibilidad de construir una atenuante por analogía en tanto que la concurrencia parcial puede excluir la idea de abuso en forma relativa. Deberá atenderse al caso concreto y la situación deberá abarcar necesariamente la proximidad por edad dispuesta en el precepto, siendo graduable el grado de desarrollo o madurez al objeto de establecer el alcance de la atenuación. Atenuante analógica que podrá tener la consideración de muy cualificada, para los supuestos en los que sin ser admisible la exoneración total, atendidas las circunstancias concurrentes, la relación entre el autor y el menor sea muy cercana a la simetría en el grado de desarrollo y madurez. La exención no podrá aplicarse a acciones típicas en las que concurra violencia, intimidación o prevalimiento.

En relación con el delito del art. 183 ter, apartado primero (*grooming*), podrá teóricamente apreciarse la exención en relación con el tipo básico, pero no respecto del agravado, que exige la concurrencia de violencia, intimidación o engaño. No podrá apreciarse esta cláusula en el delito del apartado segundo del art. 183 ter (*sexting*), por ser incompatible el «consentimiento libre» que se exige en el art. 183 quater con el «embaucamiento» propio de este tipo.

– *Circular 2/2017, sobre el ingreso no voluntario urgente por razón de trastorno psíquico en centros residenciales para personas mayores*

Responde esta circular a la necesidad de fijar unas pautas de actuación en este tipo de intervenciones judiciales, en tanto que es una cuestión examinada recientemente por el Tribunal Constitucional, así como a despejar las dudas de interpretación observadas en la práctica respecto a la Instrucción 4/2016, de 22 de diciembre, *sobre las funciones del Fiscal delegado de la especialidad civil y de protección jurídica de las personas con discapacidad de las CC.AA.,* y al importante volumen de trabajo que generan en Juzgados y Fiscalías.

Se exhorta a los Sres. Fiscales para velar porque se respete la garantía judicial y el proceso contradictorio en los internamientos involuntarios por razón de trastorno psíquico en centros residenciales para

mayores dependientes, indicando que los internamientos urgentes que no cumplan las exigencias materiales y procesales no pueden ser objeto de «regularización». No obstante, tal imposibilidad no implica que no pueda reiterarse la petición (siempre que el afectado se encuentre en libertad) ni que no existan otros títulos que permitan mantener la permanencia en el centro residencial, en tales casos se ha de valorar especialmente la situación personal del afectado a la hora de pronunciarse sobre el cese efectivo de la estancia en el establecimiento.

En cuanto a la hora de solicitar o informar sobre la adopción de medidas de protección, se deberá tener presente especialmente la necesidad de evitar lesiones al derecho a la vida y a la integridad física de la persona afectada, tomando en consideración la doctrina del TEDH sobre el art. 2 CEDH y partiendo de que el abandono de una persona con discapacidad necesitada de protección puede ser constitutivo de delito del art. 229 CP. También se deberá valorar especialmente el principio de libertad de elección y el derecho de protección social, dentro del marco de los arts. 49, 50 y 14 CE, conformidad con lo dispuesto en la LGDPD.

Para los casos en los que las personas mayores hubieran iniciado el ingreso en el centro residencial de forma voluntaria, dicho establecimiento tiene consideración de domicilio a efectos legales. La situación de demencia sobrevenida transforma el internamiento en involuntario, debiendo ser objeto de control judicial, es por ello que los Sres. Fiscales, en sus visitas de inspección, comprobarán que se cumpla esta garantía.

El internamiento involuntario de personas mayores por razón de trastorno psíquico puede realizarse en establecimientos sanitarios, asistenciales o mixtos. Cada sistema tiene sus propios criterios de definición de lo que constituyen situaciones de urgencia por lo que la interpretación del término «urgente», se ceñirán al contexto en que se realiza la intervención, rechazando interpretaciones indebidamente restrictivas.

La obligación de informar de los motivos de la detención es exigencia de los arts. 5.2 CEDH, 9.2 PIDCP y 17.3 CE, constituyendo deber del órgano judicial realizarla, algo que los Sres. Fiscales deberán comprobar en todos los procedimientos de esta índole. Por otra parte, la información de derechos comportará, entre otros extremos, los concernientes a la designación de Letrado y Procurador.

En los casos de internamiento de personas que presenten capacidad modificada judicialmente o por modificar y se encuentren en posible situación de especial vulnerabilidad, debe valorarse, en todo caso, si son procedentes medidas de protección jurídica en atención a

su situación personal, debiendo en tales casos instarse por los Sres. Fiscales la actuación de los órganos judiciales, oponiéndose a toda interpretación que demore u obstaculice la intervención de oficio.

Toda medida de protección jurídica que comporte privación de libertad deberá ser acordada con las garantías de los arts. 763 LEC y 5.1.e) CEDH, medida que podrá ser acordada *dentro de* cualquier proceso civil o penal, debiéndose entender que ha de ser en procedimiento contradictorio.

El incumplimiento de las garantías del internamiento urgente adoptado por los responsables de los centros dará lugar a la declaración de vulneración del derecho, a la imposibilidad de regularización de tal período de privación de libertad y a la posible exigencia de responsabilidades, pero en ningún caso podrá suponer peligro o perjuicio para las personas cuyo derecho se ha visto vulnerado, debiéndose oponer los Sres. Fiscales a cualquier interpretación que obstaculice la intervención judicial inmediata en evitación de peligros o perjuicios a las personas afectadas.

En cuanto al procedimiento en cuyo seno pueden adoptarse medidas de protección *ex officio*, se entiende que, por lo general, se acordarán en el propio procedimiento del art. 763 inicialmente abierto (considerando que las medidas de protección ex arts. 216 y 158 CC constituyen un título legítimo distinto al derivado del internamiento por razón de urgencia acordado por los responsables del centro) o en el de incapacidad (bien como medida cautelar o bien en sentencia definitiva), pudiendo solicitarse por el Fiscal la intervención judicial en cualquiera de ellos.

Se considera que la intervención judicial no admite demoras, por lo que se deberá promover ante los órganos jurisdiccionales la efectiva aplicación de este principio de manera inmediata.

La necesidad del control judicial de la privación de libertad no implica necesariamente la modificación judicial de la capacidad. Esta opción sólo puede justificarse, conforme a los criterios internacionales de necesidad y proporcionalidad, cuando sean exigibles medidas de apoyo que excedan del acto puntual y precisen de un contexto de protección estable, debiendo desecharse toda interpretación formalista que no respete lo anterior, por constituir práctica contraria a la CDPD.

En los casos en que se estime que, pese a concurrir causa del art. 200 CC, no existe motivo para interponer la demanda, por resultar innecesaria o desproporcionada, y se haya acordado el internamiento en fase cautelar previa (art. 762 LEC), los Sres. Fiscales –tras dictar el correspondiente decreto en las diligencias preprocesales– interesarán del Juz-

gado el cese de la medida cautelar y, en su caso, el mantenimiento de la situación de internamiento como medida autónoma de protección jurídica, conforme a los arts. 158, 216, 303 y 304 CC, cuya vigencia puede prolongarse «mientras se mantenga la situación de guarda de hecho».

– *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* (*)

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».

Se indica qué se ha de entender por datos personales, en tanto que en el art. 197.4.º b) se incorpora una nueva circunstancia agravatoria cuando los hechos sancionados en los párrafos 1.º y 2.º del mismo art. se lleven a cabo mediante la utilización no autorizada de datos personales de la víctima. A estos efectos, se ha de entender por datos personales 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.

El art. 197.7 CP recoge una nueva figura delictiva que sanciona penalmente la divulgación a terceros de imágenes o grabaciones

(*) Este borrador ha sido elaborado por la Unidad de Criminalidad Informática.

audiovisuales de una persona que, aun obtenidas con su consentimiento, se difunden, revelan o ceden sin su anuencia, lesionando gravemente su intimidad personal, entendiéndose por tales 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. Este 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.

Se ha de entender que no hay autorización del afectado cuando ésta no conste, 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.

Tratándose de 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.

El autor del delito del art. 197.7 también puede 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.

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 2.º y el art. 189.1.º 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.

Respecto al delito de acceso ilegal a sistemas informáticos (art. 197 bis 1.º) se señala que su reubicación sistemática 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.

Se considera que en la práctica será frecuente la concurrencia de este tipo, acceso ilegal a sistemas, con cualquiera de las conductas previstas en el artículo 197 n.º 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 con-

curso 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 1.º 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.

En cuanto al delito de interceptación ilegal de datos informáticos (art 197 bis 2.º) se entiende que 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 197.1.º– 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.

La ubicación de este delito en el nuevo art. 197 bis.2.º, 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.2.º y los delitos del artículo 197.1.º, 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 8.3.º 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 197.1.º Ahora bien, en el supuesto de que la interceptación ilegal (art 197 bis.2.º) concurra con alguna de las conductas ilícitas contempladas en el art. 197.2.º habrá

de apreciarse un concurso medial, del art 77 CP por las mismas razones y con las salvedades expuestas a propósito de la concurrencia del artículo 197 bis.1.º con esta misma conducta.

En cuanto al delito de abuso de dispositivos (art. 197 ter) se indica que 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.

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, 1.º y 2.º 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 men-

cionados, circunstancia que habrá de acreditarse en cada supuesto, atendiendo a los elementos, pruebas o indicios existentes. 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 LO 1/2015 traslada al art. 197 quáter 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 quáter 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.

Se indica que, dada la ubicación de los nuevos tipos penales, les será de aplicación la previsión del art. 201 CP por lo que 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. Exigencia que se estima 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.

En referencia a la circunstancia que agrava la pena prevista para el delito de daños informáticos (art. 264.2.2.º 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. 264.2.2.º 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.

En cuanto a la circunstancia del art. 264.2.3.ª 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.

La agravación del art. 264.2.4.ª 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. Por otra parte, la agravación específica prevista en el apartado 3.º 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, se deberá tomar en consideración el análisis efectuado a propósito de la aplicación de la circunstancia similar en los delitos de descubrimiento y revelación de secretos.

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. 8.1.º 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 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.

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.

El art. 264 bis 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. 264.1.º 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. 264.1.º 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 regulado en el art. 264 ter presenta idéntico contenido al del art. 197 ter, analizado en el marco de los delitos de descubrimiento y revelación de secretos 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.

– *Consulta 1/2017, sobre las acciones típicas en el delito de atentado*

Se resuelve sobre el criterio a seguir en la interpretación del delito de atentado, tipificado en el art. 550 CP, más concretamente, si la intimidación grave, considerad de forma autónoma y no vinculada a la resistencia, puede subsumirse en el tipo de atentado.

Se considera que la intimidación grave ha dejado de ser, tras la reforma operada por la LO 1/2015 una modalidad comisiva autónoma del delito de atentado. En cuanto a la conducta de acometimiento, recogida como conducta típica en el art. 550.1CP puede abarcar los supuestos de grave intimidación, cuando supongan un acto formal de iniciación del ataque o un movimiento revelador del propósito agresivo.

En el resto de supuestos para que la intimidación grave pueda subsumirse en el tipo del art. 550.1 CP debe orientarse a oponer resistencia grave a la autoridad, sus agentes o funcionarios públicos, por lo que cuando no sea un modo de resistencia no será constitutiva de delito de atentado. Los supuestos en los que la intimidación no sea equiparable al acometimiento podrán ser constitutivos de un delito de amenazas.

Se dispone que, como calificación alternativa, cuando se aprecie que la intimidación es susceptible de integrar el acometimiento y por tanto el delito de atentado se, incluirá, si existen dudas sobre la correcta subsunción, la calificación como delito de amenazas del art. 169 CP o, en su caso, como amenazas terroristas del art. 573 CP, a fin de sellar espacios de impunidad. Esta misma pauta será aplicable cuando se califiquen los hechos como atentado en su modalidad de intimidación grave con resistencia grave y existan dudas en la subsunción de la conducta.

La protección dispensada a los sujetos pasivos comprendidos en el art. 554 CP, no puede ser superior a la de los del art. 550 CP, por lo que, en todo caso, para calificar de atentado, será preciso que concurran las conductas previstas en este último precepto.

– *Instrucción 1/2017, sobre la actuación del fiscal para la protección de los derechos al honor, intimidad y propia imagen de menores de edad con discapacidad ante los medios de comunicación audiovisual*

Nace esta instrucción con el firme propósito de fijar pautas de actuación dirigidas a evitar la utilización por parte de algunos medios de comunicación de imágenes, informaciones o datos de identidad de menores en perjuicio de sus derechos e intereses. Se recuerdan actuaciones previas de la Fiscalía en este sentido, como son el *Convenio de colaboración entre la Fiscalía General del Estado y el Comité Español de*

Representantes de Personas con Discapacidad en materia de derecho de protección de la imagen de las niñas y niños con discapacidad en los medios de comunicación el 20 de noviembre de 2012, o las directrices impartidas por la Unidad de Menores de la FGE a los Fiscales especialistas (Dictamen n.º 3/2013, del Fiscal de Sala Coordinador de Menores).

En consonancia con tales antecedentes, se dispone que se deberá analizar la aparición de niños y niñas con discapacidad en los medios de comunicación audiovisual partiendo de la protección reforzada que ha de dispensarse en tanto menores de edad, por un lado, y personas con discapacidad, por otro. Por ello, aunque generalmente proceda la anuencia a la realización del programa, habrá que ponderar siempre si es necesario un control de su contenido y si el mismo ha de realizarse antes o después de la emisión.

Como criterios para valorar este tipo de emisiones, se establecen siguientes pautas: mantiene plena vigencia los criterios contenidos en la Instrucción 2/2006 sobre *el Fiscal y la Protección del Derecho al Honor, Intimidad y Propia Imagen de los Menores*. Tales criterios se aplicarán, tras las tareas de comprobación de los contenidos que exigen los arts. 3 LO 1/1982 y 4 LOPJM; la gravedad de las intromisiones en los derechos de los menores con discapacidad debe ponderarse a partir de la evolución producida en el seno de la autorregulación de contenidos televisivos e infancia y del derecho administrativo sancionador de carácter estatal y autonómico.

El marco de los contenidos intolerables que justificaría el ejercicio de acciones judiciales por parte del Fiscal se define desde la doble óptica de: los actos de intromisión ilegítima en los derechos fundamentales de cualquier persona menor de edad, y de los actos de discriminación en el tenor de la LGDPD.

En caso de que la emisión (cualquiera que sea su formato) no contemple contenidos intolerables, pero pueda verse afectada la imagen social de los niños y niñas con discapacidad por la actuación de los medios de comunicación por no responder a los criterios que exige la Convención sobre los Derechos de las Personas con Discapacidad, los Sres. Fiscales se abstendrán del ejercicio de acciones judiciales. No obstante, a través del Fiscal Delegado de Menores, se deberá poner el caso en conocimiento de la Unidad de Menores de la FGE al objeto de su correspondiente comunicación al CERMI para que, por el mismo, se procuren las restantes medidas alternativas para la plena eficacia del derecho fundamental.

Para facilitar la labor de la Comisión de Seguimiento creada conforme al Convenio de colaboración entre la FGE y el CERMI, los Sres. Fiscales comunicarán a la Unidad de Menores de la FGE los

casos relativos a programas cuyos contenidos o formas de presentación revistan características especiales o alguna complejidad.

Finalmente, se dispone que el despacho de estos asuntos corresponde a las Secciones de Menores de las Fiscalías Provinciales.

– *Instrucción 2/2017, sobre procesos incoados a raíz de la deducción de testimonios de una causa principal.*

En los supuestos de iniciación de un proceso penal partiendo de informaciones o datos procedentes de otra causa, sobre la base de unos indicios de delito obtenidos en el curso de una intervención de comunicaciones previa, si el Juez instructor no lo hace de oficio, se indica a los Sres. Fiscales que deberán instar que se unan al segundo proceso los correspondientes testimonios del procedimiento de origen. Esta diligencia habrá de interesarse desde el primer momento, especialmente cuando las defensas de los acusados hayan impugnado la diligencia de intervención de las comunicaciones.

En todo caso, cuando se formula el escrito de acusación, se deberá comprobar si efectivamente constan los testimonios de la causa matriz. En caso contrario se deberá instar su práctica.

En cuanto a qué deban considerarse testimonios a incorporar, se indica que serán en cada supuesto concreto todos los testimonios de los particulares necesarios para acreditar la legitimidad de la injerencia. Como mínimo habrán de incorporarse la solicitud inicial para la adopción de la medida, la resolución judicial que la acuerda y todas las peticiones y resoluciones judiciales de prórroga recaídas en el procedimiento de origen, así como el resultado concreto de las diligencias practicadas en la causa matriz que fundamente la apertura de la causa derivada.

Estas directrices serán también aplicables cuando en la causa matriz se hubiera acordado cualquier otra diligencia de investigación restrictiva de derechos fundamentales y se pretendiera utilizar sus resultados en un ulterior procedimiento.

– *Instrucción 3/2017, sobre documentación de las diligencias sumariales de naturaleza personal*

Tras la LO 7/2015, de 21 de julio, por la que se modifica la *Ley Orgánica 6/1985, de 1de julio, del Poder Judicial,* proclama, mediante la reforma del apartado primero del art. 230 LOPJ, la obligación de Juzgados, Tribunales y Fiscalías de utilizar «cualesquiera medios téc-

nicos, electrónicos, informáticos y telemáticos, puestos a su disposición para el desarrollo de su actividad y ejercicio de sus funciones», se proporciona rango orgánico a elementos esenciales del marco normativo prefigurado en la Ley 18/2011, de 5 de julio, *reguladora del uso de las tecnologías de la información y la comunicación en la Administración de Justicia*, en lo que concierne a la obligatoriedad de uso de los medios tecnológicos (art. 8), eficacia transversal complementadora de las leyes procesales (Disposición adicional séptima) y aplicabilidad al Ministerio Fiscal (Disposición adicional novena).

Se destaca que, esta obligatoriedad del uso de medios tecnológicos en la Administración de Justicia, ya había tenido plasmación procesal en la Ley 1/200, de 7 de enero, de Enjuiciamiento Civil, así como en la Ley 13/2009, de 3 de noviembre, *de reforma de la legislación procesal para la implantación de la nueva Oficina Judicial,* y la Ley 42/2015, de 5 de octubre, *de reforma de la Ley 1/2000, de 7 de enero, de Enjuiciamiento Civil.*

En el contexto de estas reformas legislativas, determinados juzgados de instrucción asumieron que el mandato del renovado art. 147 LEC era de aplicación supletoria al proceso penal, con expresa invocación del art. 4 LEC, y pasaron a documentar de manera ordinaria las diligencias sumariales de naturaleza personal (testificales, periciales, así como declaraciones de procesados e investigados) mediante los sistemas electrónicos de videograbación instalados en sus salas de vista, así lo que es un complemento eficaz del acta escrita pasa a convertirse en su sustitutivo a todos los efectos. Por esta interpretación, la LEC pasaba ser norma supletoria a principal, derogando el régimen singular de documentación establecido en la LECrim.

Se rechaza que en el ámbito de la instrucción penal no se pueda dar forma escrita a las actas electrónicas obtenidas de los sistemas técnicos de grabación habilitados en los Juzgados de Instrucción: en primer lugar, la diligencias sumariales sólo pueden considerarse actuaciones orales en un sentido lato, no técnico; y, en segundo lugar, ni la LO 7/2015, ni ninguna otra norma con rango de ley, ha reformado las múltiples disposiciones de la LECrim que aluden a la documentación de los actos de instrucción mediante acta escrita, su vigencia sólo puede negarse si se acredita una evidente incompatibilidad de contenidos entre la norma advenida y las disposiciones de la LECrim, incompatibilidad que en este caso no se produce.

Se apunta que una interpretación rigorista de las nuevas normas que regulan el uso de las tecnologías de la información en la Administración de Justicia puede crear un entorpecimiento o restricción de desenvolvimiento de los medios de prueba en el acto del juicio oral.

Asimismo, se destaca que el acta escrita es el medio más eficaz para concretar las citas en asuntos de cierta complejidad y que una prohibición absoluta de documentación escrita de los actos sumariales redundaría en perjuicio de las posibilidades de defensa de las partes.

Se concluye que el art. 230.1 LOPJ, desde la entrada en vigor de la LO 7/2015, acaecida el día 1 de octubre de 2015, ha generalizado el mandato de utilizar los medios técnicos puestos a disposición de la Administración de Justicia, por lo que se ha de estimar que en su ámbito de aplicación han quedado comprendidos los actos de instrucción penal de naturaleza personal (declaraciones de procesados, investigados, testigos y peritos).

El art. 230.2 LOPJ considera que las grabaciones videográficas que reúnan los requisitos técnicos de integridad y autenticidad exigidos por la Ley son documentos originales, por lo que pueden suplir eficazmente al acta escrita prevista en la LECrim para la documentación de las diligencias sumariales.

La prohibición de transcribir en soporte escrito las grabaciones videográficas recogida en el art. 230.3 LOPJ no alcanza, sin embargo, a las diligencias sumariales, por no estar comprendidas en su supuesto de hecho.

Se dispone que, cuando se estime necesario por los Sres. Fiscales para preparar adecuadamente la prueba, interesarán de forma razonada del Juzgado la documentación escrita de las diligencias sumariales. Si su petición se viese denegada, podrán hacer uso de los recursos habilitados en la LECrim para hacer valer su derecho a la tutela judicial efectiva (art. 24.1 CE) y de defensa, en la modalidad de utilización de medios de prueba eficaces y pertinentes (art. 24.2 CE).