LA CIRCULAR 3/2017 DE LA FISCALÍA GENERAL DEL ESTADO

SOBRE DAÑOS INFORMÁTICOS Y EL DELITO DEL ART. 197 CP

El **21 de septiembre,** se firmó por el Fiscal General del Estado **la nueva 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**».

DELITOS DE DESCUBRIMIENTO Y REVELACIÓN DE SECRETOS

Nueva circunstancia agravatoria del art. 197.4° b) CP

Se incorpora, en el art. 197.4° b), **una nueva circunstancia agravatoria** cuando los hechos sancionados en los párrafos 1° y 2° 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

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.

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.

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 resultarán atípicas si hubieran accedido a la difusión todas y cada una de ellas.

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.

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.

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)

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.

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 ídem, 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)

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.

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 8.3° 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°.
Ahora bien, en el supuesto de que la interceptación ilegal que estamos examinando (art 197 bis 2°) concurra con alguna de las conductas ilícitas contempladas en el art. 197.2° 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 1° con esta misma conducta.

EL DELITO DE ABUSO DE DISPOSITIVOS (ART. 197 TER)

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° y 2° 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.

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.

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

En referencia a la circunstancia prevista en el art. 264.2. 2° 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.

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.

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.

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 causa 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)

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)

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 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. 264.1° 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 operatividad o al funcionamiento del sistema informático en su conjunto.

EL DELITO DE ABUSO DE DISPOSITIVOS (ART. 264 TER)

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.